U.S. Department of Justice
National Institute of Corrections

Correctional Technology: A User's Guide

National Institute of Corrections

Larry Solomon, Deputy Director

Susan M. Hunter, Chief, Prisons Division

Anna Z. Thompson, Project Monitor

Correctional Technology:

A User's Guide

Carol Cole Kichen

James Murphy

Robert B. Levinson

American Correctional Association
Laurel, Maryland

November 1993

This document was prepared under grant number 91P07GHM9 from the National Institute of Corrections, U.S. Department of Justice. Points of view or opinions stated in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

Table of Contents

Acknowledgements

Attempting to conduct a nationwide project dealing with correctional technology required the assistance of many people. The authors want to extend their thanks to those who made the successful completion of this project possible.

In particular, we would like to express our appreciation to the Advisory Panel. Their comments on the design of this study, their help in the development of the seven survey questionnaires, and their review of study drafts were indispensable to the successful completion of the project.

Advisory Panel Members

- **Jon P. Galley,** Warden, Roxbury Correctional Institution, Hagerstown, Maryland
- **Dave Moore,** Office of the Inspector General, Oklahoma Department of Corrections, Oklahoma City, Oklahoma
- **Margaret Moore,** Executive Director/Facilities Activation, Pennsylvania Department of Corrections, Camp Hill, Pennsylvania
- **Larry Small,** Correctional Administrator, Design Development Review Unit, California Department of Corrections, Sacramento, California
- **Frank Sheridan,** Director, Facilities Planning, New York State Department of Correctional Services, Albany, New York
- **Charles N. Wimer, Jr.,** Chief of Communications, Federal Bureau of Prisons, Washington, D.C.

In addition, we would like to express our appreciation to the institutional staff who gave so unstintingly of their time while we conducted onsite visits:

William L. Callahan, Superintendent (and staff), McNeil Island Corrections Center, Steilacoom, Washington

Peter Carlson, Warden (and staff), Federal Medical Center, Rochester, Minnesota

Joe Crabtree, Warden (and staff), Federal Correctional Institution, Sheridan, Oregon

Gary J. Hilton, Assistant Director (and staff), Division of Adult Institutions, New Jersey Department of Corrections, Trenton, New Jersey

Stan Repko, Deputy Director (and staff), Division of Policy and Planning, New Jersey Department of Corrections, Trenton, New Jersey

Eldon Vail, Superintendent (and staff), Washington Corrections Center for Women, Gig Harbor, Washington

Carl Zenon, Superintendent (and staff), Oregon State Correctional Institution, Salem, Oregon

We also received excellent support from a number of individuals who assisted the project not only by reviewing drafts for technical accuracy, but also by referring us to specialized sources of information:

Resource individuals-

Randall Atlas Ph.D., AIA, President, Atlas Safety & Security Design, Inc., Miami, Florida

Povl Boesen, Engineer, Kitchell CEM, Phoenix, Arizona

Tom Cage, Physical Plant Manager, Oregon State Correctional Institution, Salem, Oregon

William R. Elmi, Sales Manager, Correctional Institutions, Harris Corporation/Digital Telephone Systems Division, New York, New York

Lori Fitzpatrick, Administrative Assistant to the Superintendent, McNeil Island Corrections Center, Steilacoom, Washington

Arthur F. Foran, AIA, President, Foran Architecture and Planning, Woodbury, New Jersey

John Geyer, AIA, Director, Patrick/NBBJ, Columbus, Ohio

Mark Giugni, Manager Marketing Communications, Harris Corporation/Digital Telephone Systems Division, Novato, California

Harry Holliday, Safety Engineer, United States Penitentiary-Lewisburg (retired), Lewisburg, Pennsylvania

Richard Holmes, Locksmith, New York Department of Correctional Services, Albany, New York

W. **L. Kautzky,** Director, Justice Programs, Henningson, Durham & Richardson, Inc., Alexandria, Virginia

LTC Lee F. Kichen, United States Army Command and General Staff College, Ft. Leavenworth, Kansas

Martha Lee, Perimeter Products, Inc., Mountain View, California

Charles B. Miller, Superintendent, Correctional Industrial Complex, Pendleton, Indiana

Dossie Mitchell, President, LOC/TEC, Rockwell, Texas

Emory Morris, Warden, Federal Correctional Institution, Sandstone, Minnesota

Carroll Montgomery, Facilities Manager, Federal Correctional Institution, Sheridan, Oregon

Harold E. Nelson, Senior Research Engineer, Building and Fire Research Lab., National Institute of Standards and Technology, Gaithersburg, Maryland

Allen Patrick, FAIA, Principal in Charge, Patrick/NBBJ, Columbus, Ohio

Captain A. E. Scamahorn, Chief of Security, McNeil Island Corrections Center, Steilacoom, Washington

Jack L. Shetter, President, Security Design, Inc., Spokane, Washington

LTC Frank E. Ward, United States Army Command and General Staff College, Ft. Leavenworth, Kansas

In addition, we acknowledge the financial support received from the National Institute of Corrections, and the helpful advice and suggestions provided by Wayne Huggins (former director, NIC), Susan Hunter, and Anna Thompson.

Carol Cole Kichen, Project Co-Director

James Murphy, Project Co-Director

Foreword

The National Institute of Corrections is convinced that corrections officials should be extensively involved in the selection of technologies that comprise an integral part of their institutions. While some studies have been completed, there is no one place to which administrators can turn for a uniform knowledge base to guide their technology decisionmaking. The lack of objective research, written in user-friendly language, forces administrators to rely on vendor-supplied information and public-relations-oriented product descriptions.

Correctional Technology: A User's ***Guide*** is meant to provide corrections administrators with a nonbiased, objective source for evaluating different correctional technologies in use today. It contains the following chapters:

- Chapter l-Perimeter Security Systems
- Chapter 2-Locks and Locking Systems
- Chapter 3-Internal Detection Systems
- Chapter 4-Monitoring and Surveillance Systems
- Chapter 5-Fire Safety Systems
- Chapter 6-Communication Systems
- Chapter 7-Management Information Systems.

The intent of this user's guide is to provide the corrections community with a set of valuable decisionmaking tools. It should help ensure that technology assists in improving the operation of the nation's prisons and jails.

Larry Solomon

Larry Solomon, Deputy Director
National Institute of Corrections

Methodology

The American Correctional Association (ACA) was awarded a grant in April 1991 by the National Institute of Corrections (NIC) entitled “Correctional Technology: A User’s Guide.” The purpose of the grant was to assess seven areas of correctional institution technology to include the following:

- Perimeter security systems,
- Locks and locking systems,
- Internal detection systems,
- Monitoring and surveillance systems,
- Fire safety systems,
- Communication systems, and
- Management information systems.

The goal of this 18-month study was to develop a user’s guide for correctional administrators that would provide the following information:

- A description, in nontechnical terms, of the types of technology in use;
- An indication of support systems and staff needed to install, operate, and service the various systems;
- Factors to be considered during the selection and planning for the use of technology; and
- Conditions under which particular technologies are appropriate or under which they may be unreliable, ineffective, or inefficient.

The project was developed in 11 stages, comprising the following:

1. A Review Committee was established and met for 3 days in May 1991 to:
    - Determine the most effective way to approach the project,
    - Decide on the types of survey questions that would have the best chance of eliciting beneficial information for administrators when they evaluate and select technologies for new facilities or retrofit older institutions,
    - Determine the organization and design for the final project report, and
    - Decide on methods for maintaining institutional anonymity in order to protect the participating institutions’ security and to obtain candid information.

2. Based on decisions made during the Review Committee meeting, a short, exploratory questionnaire was developed to determine the level of technology use in adult facilities in the United States and at the federal level in Canada.

This initial questionnaire was short. It included a brief section that provided a profile of each institution and a second section that asked respondents to indicate which systems they had. In addition, facilities were asked if they would participate in the more detailed phase of the project.

The questionnaire was sent to 807 institutions. The number of responses was 472 (58 percent); of these 465 (99 percent) agreed to participate in a more comprehensive survey to examine the effect of technology on institution operations.

3. As replies to the initial questionnaires were received, they were entered into a database designed to compile the information necessary to select the sample population of facilities-those that would be invited to participate in the more detailed phase of the project.

Selection criteria for institutions included in the final sample consisted of, but were not limited to, average daily population, level of security, age of physical plant, geographic location (boundaries followed those established by the Bureau of Justice Statistics), gender of inmates, and types of technology used. The following decisions were made:

- Each of the seven technology-specific survey instruments would be sent to approximately 50 institutions, and
- Because of the length of the surveys, no single facility would be asked to respond to more than three technology areas (i.e., survey instruments).

4. A literature search was conducted to obtain information on the seven areas of technology to be studied. Information was collected from the National Institute of Justice/ National Criminal Justice Reference Service, the National Institute of Corrections Information Center, and the library at the American Correctional Association.

Additional information was provided by vendors and experts in each of the seven technology areas being assessed. Each survey instrument was designed to elicit both multiple-choice and open-ended responses to one of the seven technology areas.

5. Seven more comprehensive survey instruments were then developed. These were submitted to the Office of Management and Budget for review and approval, in accordance with the Paperwork Reduction Act and 5 CFR 1320.

6. As the surveys were developed, their content was reviewed for comprehensiveness and accuracy by experts from various agencies and the private sector including:

- Architects,
- Corrections practitioners,
- Engineers,
- Manufacturers,
- Military personnel,
- National Aeronautics and Space Administration (NASA),
- National Institute of Standards & Technology,
- National Security Agency (NSA),
- U.S. Secret Service, and
- Vendors.

These reviewers helped to determine whether the survey instruments would elicit the information needed to develop the final guide. They also helped to ensure that the items were worded properly and that unnecessary or redundant questions were not being asked.

In addition to being reviewed by these experts, the surveys were field-tested in a variety of institutions in several states to determine:

- How staff in participating institutions would react to the survey instruments,
- If the terminology was universal (that is, would it be understood by staff in facilities in any geographic area and at all levels of security?), and
- Whether the time required to complete any one survey would be too burdensome.

7. Information was sent to correctional administrators to introduce the project, explain how it would be accomplished, and ask for their support.

8. When the sample population of facilities was selected, the administrator of each jurisdiction was notified as to which institutions had been selected from that system and which technology survey(s) each facility would receive.

The administrators were assured that institutional anonymity would be maintained and that the final user's guide would display aggregate data only.

Each selected facility was notified as to which survey instrument(s) it should be expecting. In addition, instructions were sent on how the surveys should be filled out. Respondents were encouraged to provide additional comments concerning any questions they felt needed to be addressed in more depth than the survey item provided for.

9. Databases were developed to provide a profile of each facility, including location, security level, manner of supervision, average daily population, year the facility was opened, and recent and planned construction or renovation.

A second set of seven databases was generated-one for each technology area. The facility profile and the technology databases were related only by a code number to maintain institutional anonymity.

10. For all of the detailed survey instruments, the return rate was 93 percent. This high proportion of responses was due, in part, to the fact that only institutions that had agreed to participate in the survey were contacted and to a continuing effort to keep participants informed of the project's progress. Response rates for each technology area were as follows:

Technology Areas	# Sent	% Returned
Fire Safety Systems	62	100%
Management Information Systems	49	96%
Perimeter Security Systems	61	90%
Locks and Locking Systems	48	88%
Monitoring and Surveillance Systems	58	86%
Internal Detection Systems	66	85%
Communication Systems	69	81%

11. The data compiled from the surveys were used (in conjunction with information obtained in follow-up interviews and site visits) to write the seven separate chapters in this user's guide-one for each area of technology. This user's guide will help administrators become more knowledgeably involved during the selection and use of these technologies.

The user's guide does not endorse any product or type of product, nor does it support one technology over another. Its intent is to provide administrators with an unbiased compilation of experiential information as supplied by their colleagues.

Chapter 1

Perimeter Security Systems in Correctional Facilities

Abstract

Correctional Technology: A User's ***Guide*** is the product of a nationwide assessment of the experience correctional administrators have had with various types of technological systems. The purpose of this guide is to provide correctional administrators with a user-friendly source of information to aid planning and decisionmaking.

For this chapter on perimeter security systems, survey questionnaires were prepared, reviewed by experts in the field of perimeter security, pilot-tested onsite, and revised in light of that input. The final version was sent to 61 correctional institutions selected to represent all areas of the country and all levels of security. Presurvey letters and follow-up telephone calls resulted in a 90 percent response rate.

No institution in the sample relied on a single perimeter security system; the average number of systems per facility was four. Perimeter patrols, towers, and video cameras were used most frequently. Redundancy was advocated (i.e., pairing technologies so that one compensates for the weakness of another). False alarms-including alarms that are caused by equipment malfunction, and "nuisance alarms," which are caused by environmental factors-were common, occurring at a several-per-month rate.

The perimeter security system solved the problem for which it was purchased in 95 percent of the sampled institutions.

Table of Contents

LIST OF TABLES

Executive Summary

In order to obtain information for this study on perimeter security systems, 61 institutions were sent survey questionnaires. Fifty-five responded, giving a 90 percent response rate. Institutions were randomly sampled but were chosen so that different security levels and geographic locations were represented. Fifty-one percent had opened since 1980. Institutions with the largest average daily population were found in the Midwest; the West had smaller facilities.

Ninety-five percent of the responding facilities were fenced. The average institution had two fences and used five coils of razor wire placed on top of the fence. In 78 percent of the cases, the perimeter was subdivided into zones. The average number of zones per facility was 16, with an average length of 124 feet.

No institution in the sample relied on a single perimeter security system; the average number per facility was four. Perimeter patrols, towers, and video cameras were most frequently used (in 69 percent, 56 percent, and 51 percent of the institutions, respectively). This type of redundancy allowed for pairing technologies so that one compensated for the weakness of another.

Nuisance alarms were reported to be caused most typically by lightning, wind, and hail. Seventy-one percent of the respondents that reported experiencing such nuisance alarms from lightning and power surges had fence-mounted, motion-sensor systems. Half of these facilities also had microwave systems that were less susceptible to this type of difficulty.

No pattern was found in the number of reported false alarms from malfunctioning equipment. The number of such alarms ranged from five a day to three a year. Commonly, several false alarms occurred each month.

This study found that when an alarm was triggered, the average institution assessed its cause within 40 seconds, typically by an armed officer (sidearms or shotgun) stationed in a standard pickup truck used as an outside-the-perimeter patrol vehicle.

For the institutions in this study, perimeter security system breakdowns tended to be few, with an average of 6 months between malfunctions. More than one-third of the respondents never had a zone failure that lasted longer than 24 hours; however, there was an average of ten zone failures per year per institution. Preventive maintenance offered a partial solution to this problem, with most maintenance and repairs being accomplished without negatively affecting institution security.

Half the institutions sampled reported being happy with their perimeter security systems. The remainder had some other technologies on their wish list, the most popular of these being motion detectors and video cameras. In 95 percent of the sampled institutions, the perimeter technology solved the problem for which it was purchased. For the remaining 5 percent, difficulties continued, as reflected in too many false alarms or because of the need for additional video cameras.

Introduction

A correctional facility is only as secure as its perimeter. The basic function of a perimeter security system is to detect, as quickly as possible, unauthorized entry into a defined area. Effective systems are difficult to bypass or override. Such systems must also be highly reliable and able to operate under adverse conditions (e.g., power failures). Additionally, perimeter security technology should not be subject to false alarms.

There are two types of technology: perimeter detectors and space protectors. Space protection devices differ from perimeter technology in that they provide volumetric (three-dimensional) coverage. Such systems as infrared, ultrasonic, and microwave can detect an intruder throughout the height, width, and length of an area.

Perimeter detectors consist of different types of switches (e.g., magnetic, vibration, or trip wires) strategically located around the perimeter of the protected region. They operate on the principle that breaking a circuit triggers an alarm. These systems are easier to circumvent than space protection technology; however, they are less susceptible to environmental problems and tend to have fewer false alarms.

Ultimately, the effectiveness of any alarm system lies in the response it commands. An alarm takes no action; it only notifies staff that action is needed. In the final analysis, all perimeter security systems are only as effective as the staff who respond to them.

Responses to the Perimeter Security/Intrusion Detection Systems questionnaire reflect the variety of institutions included in the sample. In all, 55 facilities replied, producing a 90 percent response rate.

The objective of this chapter is to provide corrections administrators with information relevant to decisionmaking about perimeter security systems technology. It includes the following:

- A description, in nontechnical terms, of the types of technology in use;
- An indication of support systems and staff needed to install, operate, and service the various systems;
- Factors to be considered during the selection and planning for the use of technology; and
- Conditions under which particular technologies may be appropriate, reliable, effective, or efficient.

This chapter contains the following:

- An overview of perimeter security systems,
- A description of the characteristics of the institutions sampled in the survey,
- An analysis of the survey findings,
- Conclusions drawn from survey results, and
- Issues to consider when evaluating a perimeter security system.

Perimeter Security Systems: An Overview

Essentially, perimeter security systems consist of either stationary or movable technology and use a variety of devices and/or procedures designed to contain an inmate population and/or detect intrusions into barrier zones.

Perimeter patrols (used by 69 percent of the respondents) consist of an armed officer who periodically drives around the outside of an institution's perimeter.

Towers (found in 56 percent of the sampled institutions), above-ground stations staffed by armed officers, are usually located around an institution's perimeter. They are positioned to give the officer a clear view of the fence/wall line.

Video cameras (used by 51 percent of the respondents) are closed-circuit television cameras (CCTV), under remote control, and positioned to provide officers in the control center a view of blind areas.

Microwave sensors (found in 45 percent of the sampled institutions) use a microwave transmitter that emits high-frequency radio waves between itself and a receiver. These radio waves form an invisible electric field whose height and width are specified by the system. Anything entering the field disturbs the waves, which are then partially reflected back to the detector. Electronic circuitry compares the transmitted frequency with the received frequency and triggers an alarm when a change is detected.

In a monostatic microwave system, a single sensor both sends and receives the waves. In a bistatic system, the sensors that transmit are different from those that receive.

These systems cover large areas at low costs, with equipment that typically is inconspicuous. On the whole, the equipment is easily maintained, though much depends on how well the sending and receiving sensors are aligned. Zones are easy to identify. Microwave links can be overlapped to form a protected perimeter around a facility.

Microwave systems work best in flat terrain where line-of-sight facility boundaries are straight. Hills or other obstructions will interrupt the beam, while ditches and valleys may provide crawl space for an intruder. There are some dead areas at the sensors because of the shape of the field, but this can be alleviated by having zones overlap. Heavy rains, objects blown into the field by the wind, and animals can all cause nuisance alarms, and snow (or other reflective surfaces) can reduce the area of effective coverage.

Fence-mounted motion sensors (used by 42 percent of the respondents) are either mechanical or electromechanical sensors that are attached to the fence and connected by electric cables. Movement of the fence sends signals through the cables to alarm devices.

Motion sensors provide a simple, economical system. Zones are easily identified. Unlike some other technologies, this system does not have to be shut down during yard maintenance. Since it attaches directly to the fence, the system requires no special site preparation; however, proper operation depends on a well maintained fence. Moving parts may wear over time and require adjustments. Sensor tape must be mounted as far off the ground as possible to maximize its effectiveness.

Taut wire (found in 25 percent of the reporting facilities) involves multiple parallel tension wires that are strung between posts and mechanical sensing switches along the top of a perimeter barrier. Tension on the wires is scientifically calibrated and any change (either more or less) closes a switch that sends a signal to the alarms. False and nuisance alarms are caused mainly by deep snow, freezing rain, or ice, but the frequency rate is very low.

Infrared sensors (used in 15 percent of the sampled institutions) are electrical devices that generate infrared light beams that form an invisible or nearly invisible field between each transmitter and receiver. The sensors are stacked vertically and are usually angled to form a crossed pattern. The technology "sees" the heat emitted by a human body that enters the field and sends a signal to the alarm system. Electronic circuitry allows sensors to differentiate between heat from a human and heat generated by such things as incandescent light bulbs.

These systems inconspicuously monitor very narrow as well as very large areas, though, like microwaves, they are best suited to a flat site with straight boundaries. Maintaining accurate alignment of sending and receiving sensors is important. Ground maintenance is not a problem for this system.

Infrared sensors are sensitive to anything that might obscure its beams, including fog, smoke, or a heavy snow fall. Coverage can also be negatively affected by reflective surfaces like snow or ponds.

Canine patrols (used in 9 percent of the responding institutions) consist of trained dogs, who with their handlers, search for contraband items, particularly drugs. Some facilities let dogs roam between perimeter fences or on the compound after lights-out.

Video motion detection (used by 9 percent of the respondents) employs special photoelectric detectors mounted on remote television cameras to sense motion within a protected area. The detectors cause a camera to focus on the area in which the motion occurred. Some form of illumination is required.

Although the area covered can be quite large, the system cannot be used independently since it requires staff to constantly monitor a screen. The technology is good for covering weak or dead spots to enhance the effectiveness of another system.

Electric field sensors (found in 7 percent of the responding facilities) consist of a two-wire system with the sensing wire located between 200 and 450 millimeters above the ground, and the field wire located approximately 1 meter above and parallel to the sensing wire. The width of the detection zone is variable. An alarm is signaled when the balance of the field is disturbed by the entry of a nonconducting object like a person.

The system is good on hilly or contoured terrain and may be free-standing or fence-mounted. Free-standing systems can cause problems for grounds crews, especially since vegetation (e.g., tall grass) must be controlled in its vicinity. Moreover, the system is expensive both to buy and install. It requires extra maintenance, and its sensor wires must be replaced every 3 years. It also has to be readjusted for temperature changes, and snow, rain, and lightning can cause false alarms.

Ported coaxial cable (used by 4 percent of the respondents) uses shielded buried cables to transmit electromagnetic energy through very small openings, creating a field sensitive to interruption. Detection depends on interruptions that cause an electrical signal (reflecting the object's mass, velocity, and length of time in the field) to be sent to an alarm.

The equipment is concealed and easily follows site configuration. Weather, air pollution, and ground vibration do not affect the system, and maintenance is minimal. However, the system is expensive to buy, install, and maintain.

False alarms may be caused by pooling water, high winds, tree roots, and moving metal objects like mowing equipment.

Seismic in-ground sensors (found in 4 percent of the responding institutions) are buried pressure/strain transducers used to detect small variations in the mechanical stress exerted on the surrounding soil by the presence of an individual passing above the sensor. The signals produced by the transducers are amplified and compared with a pre-established threshold. If the signal exceeds this limit, an alarm occurs.

The system works well in any terrain and is especially good in warm climates with little rain. However, it has a high false-alarm rate in response to vehicles, hail, or heavy snow.

Sample Characteristics

Ninety percent of the 61 facilities invited to help provide a clear picture of institutional responses to perimeter security replied. Their geographic distribution, based on specific boundaries established by the Bureau of Justice Statistics, was wide: 11 were in the Northeast, 14 in the South, 14 in the Midwest, 13 in the West, and 3 in Canada.

Of the 55 respondents (52 U.S. and 3 Canadian), 8 were minimum security, 21 were medium security, 8 were maximum security (long-term, difficult inmates), and 18 were mixed security (i.e., no inmate group, in terms of security needs, exceeded two-thirds of the facility's population). One-third of the facilities had a population under 500, while 40 percent regularly had over 1,000. Fifty-one percent were opened since 1980.

LOCATION AND SECURITY LEVELS

Table l-l shows the geographic distribution of the 52 U.S. survey respondents. Most responding institutions were located in the South and Midwest (27 percent each), followed by the West (25 percent), and the Northeast (21 percent). Table 1-2 shows the levels of security of the U.S. respondents.

Statistical analyses of data used to develop Tables l-l and 1-2 reveals a nonsignificant (N.S.) relationship between the number of respondents in each security category and geographic location.* In other words, there was random geographic distribution of the sample institutions.

Table 1-1
Location of Sample Facilities

Location	n	%
Northeast	11	21
south	14	27
Midwest	14	27
West	13	25
Total*	52	100

. Excludes three additional Canadian facilities that responded to this survey.

AGE OF SAMPLE FACILITIES

All 55 respondents (including the three Canadian facilities) provided the date when their institutions were opened (see Table 1-3). Fifty-one percent were relatively new, built since 1980, while three were opened prior to 1900.

* For four security levels, x^2 = 12.594; df=9; N.S. A comparison conducted without the mixed category yielded x^2 = 6.591; df=6; N.S.

Table 1-2
Security Level of Sample Facilities

Security Level	n	%
Minimum	8	15
Medium	19	37
Maximum	8	15
Mixed*	17	33
Total'	52	100

- Inmate population was less than two-thirds in any security category.

† Excludes three additional Canadian facilities that responded to this survey.

Table 1-3
Date Facilities Opened

	n	%
Before 1900	3	6
1900-1939	9	16
1940-1979	15	27
1980-Present	28	51
Total	55	100

POPULATION SIZE OF SAMPLE FACILITIES

Facility size by average daily population (ADP) is shown in Table l-4. Table l-5 breaks out the 52 U.S. facilities by region and ADP. Table l-4 shows that 31 percent of the total sample had an ADP under 500. Table l-5 shows:

- Only 1 (9 percent) of the 11 Northeast facilities had an ADP of fewer than 500 inmates.
- Of the total of 16 institutions with an ADP of under 500, 8 (50 percent) were in the West.
- Forty-one percent of the 22 institutions with an ADP over 1,000 were located in the Midwest.

Table 1-4
Average Daily Population

Population	n	%
Under 500	16	31
500-999	14	27
1000+	22	42
Total*	52	100

*Excludes three Canadian facilities that responded to this survey.

Table 1-5
ADP by Region

Population	Northeast	south	Midwest	West	Total
Under 500	1	4	3	8	16
500-999	5	6	2	1	14
1000+	5	4	9	4	22
Total'	11	14	14	13	52

* Excludes three Canadian facilities that responded to this survey.

Chi square analysis of the data used to develop Tables 1-4 and 1-5 reveals a statistically significant relationship between size (ADP) and location: Larger facilities were located in the Midwest, smaller ones in the West.*

* $X^2 = 14.096$; df=6;p < .05.

Survey Findings

TYPE AND MIX OF PERIMETER SECURITY SYSTEM USAGE

Table l-6 shows that among the 55 responding institutions, three approaches to perimeter security were used in more than half of the sampled institutions: perimeter patrols (69 percent), towers (56 percent), and video cameras (51 percent).

No respondent relied on a single system; invariably several were combined. The average number of systems per institution was 3.7; the range was from a high of seven to a low of two. The most frequent number of systems per institution was four.

Table 1-6
Perimeter Security Systems - Usage

	No. of Facilities	%*
Perimeter Patrols	36	69
Towers	31	56
Video Cameras	28	51
Microwave Sensors	25	45
On-Fence Motion Sensors	23	42
Taut Wire	14	25
Infrared Sensors	8	15
Video Motion Detection	5	9
Canine Patrols	4	9
Electric Field Sensors	4	7
Ported Coaxial Cable	2	4
Seismic In-Ground Sensors	2	4
Other	13	24

• The total percentage exceeds 100 because a number of respondents reported using more than one perimeter security system.

Mobile Systems

Perimeter Patrols. Usually, officers in roving vehicles patrolled the perimeter of the respondents' institutions (83 percent) (see Table 1-7). Alternatives were officers on foot (36 percent), in a stationary vehicle (23 percent), or with dogs (9 percent).

As shown in Table 1-8, the patrol vehicle might be a standard pickup (55 percent), a four-wheel-drive vehicle (46 percent), or a sedan (28 percent). Vans, electric golf carts, or officers' own cars were also used. Patrolling was done outside the fence more often (89 percent) than inside it (23 percent).

The patrolling officers were usually armed (76 percent) and often with more than one type of weapon. Favorites were sidearms (75 percent) and shotguns (74 percent), with rifles (18 percent) a distant third choice (see Table 1-9).

Generally, multiple types of perimeter security systems were used. In more than half the facilities (54 percent), the systems were installed at the same time. Where they were added later (46 percent of the cases), the most recent one was installed either to increase security whether or not there was an escape, replace an obsolete system, secure additional fences, or save wear on the fence by installing microwave at the sally-port.

Canine Patrols. Using dogs to patrol a corrections facility was reported by 9 percent of the respondents. Often they were deployed at night between perimeter fences.

Table 1-7
Type of Perimeter Patrols

	No. of Facilities	%*
Roving Vehicle	39	83
Officer on Foot	17	36
Stationary Vehicle	11	23
Canine	4	9
Other	3	6

* The total percentage exceeds 100 because a number of institutions reported using more than one type of perimeter patrol.

Stationary Systems

Fences. Although there were walls around one in five of the reporting facilities, 96 percent were fenced. Institutions averaged two fences. Nine out of ten of the respondents used razor wire with an average of 5 coils each (the range was from 1 to 15).

Razor Wire. All facilities but one (98 percent) placed razor wire on top of their fences, 55 percent deployed it between fences, 36 percent placed it inside the interior fence, and 13 percent put it on the inside wall (see Table 1-10). Other razor wire locations were at the bottom of fences, on building comers, on top of inside gates, and over buildings that divided fences.

Razor wire was usually attached with wire ties (72 percent), but wire rings (17 percent) and angle hangers (13 percent) were also used; one facility used fiber-glass rods.

Table 1-8
Type of Patrol Vehicle

	No. of Facilities	%*
Standard Pickup Truck	22	55
4-Wheel Drive	18	46
Sedan	11	28
Vans	6	15
Station Wagons	3	8
Other	3	8

. The total percentage exceeds 100 because a number of institutions reported using more than one type of patrol vehicle.

Table 1-9
Patrol Officers' Weapons

	No. of Facilities	%*
Sidearms	26	75
Shotguns	25	74
Rifles	6	18
Other	6	18

* The total percentage exceeds 100 because a number of institutions reported patrol officers used more than one kind of weapon.

Alarms. For most institutions, the activating of a single alarm was enough to cause immediate response. But a few facilities declared an emergency only when ***all*** systems were triggered. Where there was more than one system, in only 21 percent of the facilities were they selected to be responsive to different triggering intrusions.

Almost all the respondents (93 percent) had dedicated power sources to backup their perimeter security systems. These could operate for an average of 108 hours (range from a low of 2 to an indefinite number of hours).

In nine out of ten sample institutions, their intrusion detection systems used a control panel or console with a status indicator. Respondents were of the unanimous opinion that the status indicators were reliable and that the alarm information coming in was easy to read. Usually the panel was located in a control center (87 percent), but occasionally it was in a tower (7 percent) or an arsenal (5 percent).

Table 1-10
Location of Razor Wire Coils

	No. of Facilities	%*
On Top of Fence	46	96
Between Fences	26	55
Inside Interior Fence	17	36
inside Wall	6	13
At Bottom of Fence	4	9
Other	6	13

* The total percentage exceeds 100 because a number of institutions reported more than one location for placing razor-wire coils.

In about one-quarter of the cases (23 percent), the control panel was mounted in a patrol vehicle. The average number of vehicles with panels was two. Where patrol vehicles had panels, there was always a backup. No matter where panels were located, intrusion detection was almost always monitored (98 percent).

Almost eight of ten facilities conducted probability-of-defeat testing. Typically, for 100 attempts, a system's alarm was triggered 99 times (one facility reported a 90 percent reliability).

Two out of three facilities tested alarm response time. Findings showed that most institutions assessed the situation within 40 seconds after an alarm was given. For the 15 facilities reporting on how many seconds' delay their perimeter barrier provided, the average was 36 seconds. The range was from a low of 2 seconds to a high of 5 minutes.

Facilities sometimes checked out alarms in more than one way (see Table 1-11). The most popular method for checking was by patrol car (71 percent), followed by video (34 percent), tower observation (34 percent), foot patrols (32 percent), and audio (26 percent).

Towers. Most facilities (71 percent) staffed their towers around the clock; while, at the other extreme, 32 percent of the reporting institutions had personnel in towers for only one shift (see Table 1-12). At one institution that did not have towers, the explanation given was:

> ***I am a firm believer that guard towers can be effectively eliminated in medium prison surroundings if a very broad perimeter was established utilizing state-of-the-art technology and perimeter patrols. Tremendous savings in manpower expenditures can be realized.***

ZONES

The average institution perimeter measured 4,712 feet, and ranged from 100 feet to more than 3 miles (18,480 feet). Seventy-eight percent of the facilities organized their perimeter security into zones. The average number of zones was 16 (range from 1 to 59). Zone lengths varied from 10 to 800 feet; the average was 124 feet. Only one in five facilities discovered dead zones in their perimeter security systems. To overcome these, they added staff, cameras, razor wire, or canine patrols.

Table 1-11
Perimeter Alarm Assessed By

	No. of Facilities	%*
Patrol Vehicle	27	71
Video	13	34
Tower Officer	13	34
Officer on Foot	12	32
Audio	10	26

* The total percentage exceeds 100 because a number of institutions reported their alarms were assessed by more than one entity.

SPECIFICATION AND INSTALLATION ISSUES

Specifications

Only 26 percent of responding facilities wrote perimeter security systems specifications on their own (see Table 1-13). Most relied at least partially on a consultant (45 percent), a vendor (37 percent), or, in the case of federal institutions, on the General Services Administration. For two of the sampled facilities there were no formal specifications.

Table 1-12
Towers - Staffing Pattern

No. of Shifts	Average No. Staffed	High No. Staffed
3	4	12
2	3	9
1	2	4

Installation

Almost eight out of ten facilities (79 percent) required the installer to supply a performance bond, and, of those that did, a similar percentage (78 percent) required the bonded installer to fix any post-installation problems that developed with the perimeter security system.

All the equipment reported on was installed according to manufacturers' directions. Nevertheless, three out of four facilities were unable to get their systems to perform after installation. In the three worst cases, it took 2 years to find and correct the problems that caused the malfunctions. In the best case, the problem was solved in just 2 days. In eight out of ten cases, no additional costs to the facilities were involved in correcting post-installation performance problems. One respondent mentioned the importance of independently testing the perimeter security equipment-in this case a motion sensor:

> ***The system was reliable when tested following vendor's instructions . . . [however facilities with similar systems] should conduct actual test cuttings of their perimeter fences. This facility had utilized the current system for the last 8 years and conducted the first actual cutting test in 1992. It failed.***

Table 1-13
Specifications for Detection System

Written By:	No. of Facilities	%*
Consultant	17	45
Vendor	14	37
Facility	10	26
Central Office	4	11
No Specifications	2	5
Other	6	17

* The total percentage exceeds 100 because a number of facilities reported that detection system specifications were written by more than one entity.

TRAINING

Although one respondent emphasized the importance of ***"adequate training regarding the function and use of the perimeter security system,"*** the plea may be falling on deaf ears. only 36 percent of the sampled facilities reported giving staff formal training on how to operate their perimeter security systems; 38 percent trained staff to maintain and repair the systems.

Operations Training

On average, 26 percent of an institution's staff (ranging from 2 percent to 80 percent) were trained to operate perimeter technology. However, the average number of training hours was 8, with a high of 80 hours and a low of 1 hour. In 86 percent of the cases, the facility did the training. Twenty-eight percent used the vendor.

Maintenance Training

Compared with instruction in how to operate perimeter security systems, training provided by the sample institutions in maintenance and repair was more comprehensive. The average number of training hours was 34 (range from a low of 8 hours to a high of 100 hours). However, the number of staff trained in repair procedures was quite low, with an average of only 3 percent (range from a three-tenths of 1 percent to a high of 10 percent).

For repairs, although facilities did train on their own (45 percent), they were more likely to go to an outside vendor (41 percent). Five percent required that staff be hired who were already trained.

Staff members trained to take care of perimeter security were likely to be technicians (78 percent), though they might also be members of the general maintenance staff (22 percent).

MAINTENANCE AND REPAIR

In 67 percent of the cases, facility staff assumed much of the responsibility for maintenance and repair, outside contractors also did a lot of this work (59 percent). The manufacturer took care of the system in 23 percent of the reporting facilities.

Topping the list of repairs needed was readjusting sensor sensitivity (24 percent), followed by repairing or replacing cameras (10 percent), conduits (10 percent), microwave heads (10 percent), and/or circuit boards (8 percent). Other repairs included replacing light bulbs, fuses, and the electronics in cameras and monitors, and repairing or adjusting audible signals.

Scheduled maintenance seemed to be a good idea. Eighty-one percent of the reporting institutions that used regular maintenance schedules said they had no problems that required repairs.

Down-Time

Equipment Break-Down. Perimeter technology did not break down often. Although one facility reported problems on an average of every 4 hours, for the rest, the average number of months between system breakdowns was 6, with a high of 12.

Most repairs could be done within an average of 14 hours. Almost all institutions had been able to keep down-time for repairs under 3 days (range to a high of 6 weeks).

Would maintenance contracts make any difference in down-time where staff was currently doing the work? Probably not, respondents decided. Only 12 percent thought maintenance contracts would reduce costs, although 29 percent thought the quality of repairs might improve with a contractor.

As for stocking spare parts, 63 percent did keep some on hand, though 92 percent found that replacement parts were readily available outside the facility.

Zone Failures. More than a third of the respondents (37 percent) never had a zone fail for more than 24 hours (the longest was six 6 weeks; average 2 to 10 days). Even though zones did not stay down for long, such failures were not uncommon. The 26 facilities responding to this question reported an average of 10 zone failures per year, with a low of 1 and a high of 50.

Of those facilities that reported zone failures, waiting for parts topped the list of causes (36 percent), with inclement weather a distant second (12 percent). Other reasons included frozen water in conduit lines (because of an unusual sequence of subzero temperatures), water damage to electronics, power supply failure, a bad zone card, faulty installation, and lack of funds for repair work. The institutions reported that most maintenance and repair could be done without negatively affecting institution security.

System Testing and Maintenance

The number of breakdowns may have some relationship to the frequency with which perimeter security equipment underwent routine testing (Table 1-14). More than half the respondents reported that they tested their whole perimeter security system weekly (34 percent) or monthly (20 percent); several reported additional visual testing either weekly (7 percent) or monthly (14 percent).

Many facilities reported testing their systems more frequently than monthly or weekly. Of those who did, 58 percent checked their perimeter security systems daily, 12 percent twice a day, 12 percent at each shift change, and 6 percent three times a day. At the other extreme, 12 percent tested only when the system malfunctioned.

Almost invariably, staff played some role in testing and maintenance (86 percent). Staff testing was supplemented, and occasionally replaced, by vendors (17 percent) or outside contractors (14 percent) (see Table 1-15).

OPERATIONAL CONCERNS

Escapes

Since their current security technology was installed, 55 percent of the facilities reported having had escape attempts. Among those that did experience such attempts, the number ranged from 1 to 12 (with average of 2). Ten attempts were successful. The in-place system alerted staff during 83 percent of the attempts.

False Alarms

There was no discernible pattern in the number of false alarms reported. One facility reported an average of five false alarms a day, and another reported three a year. Commonly, several false alarms occurred each month.

Most false alarms could be traced to equipment (57 percent) or installation (29 percent) problems. Other factors were static electricity, an overly sensitive system, and neglecting weed control.

Table 1-14
Perimeter Security Maintenance/Testing Schedule

	No. of Facilities	%*
Every Shift	3	9
Twice Daily	3	9
Daily	6	17
weekly	12	34
Monthly	7	20
Quarterly	2	6
Semiannually	3	9
Annually	3	9
Randomly	5	14
Other	5	14

* The total percentage exceeds 100 because a number of institutions reported that they perform perimeter security maintenance on more than one schedule.

Table 1-15
Perimeter Maintenance Performed By

	No. of Facilities	%*
Staff	30	86
Vendor	6	17
Contractor	5	14
Other	3	9

* The total percentage exceeds 100 because a number of institutions reported that perimeter maintenance was performed by more than one kind of entity.

Nuisance Alarms

This type of false alarm, often caused by weather or animals, was reported by 95 percent of the respondents.*

Seventeen facilities reported daily nuisance alarms-from as few as 2 to as many as 30, with an average of 9. Other institutions averaged 3 nuisance alarms a week, while one reported as many as 250 per month. They occurred often enough that 39 percent of the sampled institutions had established an acceptable standard number of nuisance alarms before becoming concerned. Eight institutions allowed a daily rate averaging 5, while others permitted no more than 2 to 4 per week. Most often (54 percent of the cases), standards were set in response to the following:

- Demands on the staff,
- A manufacturer's suggestion,
- The probability of detection, or
- A realistic assessment of the security risks.

In over a quarter of the facilities (26 percent), nuisance alarms were treated with the same high level of concern as any other alarm.

Costs

Were perimeter technology systems cost-effective? Asked how many additional officers would be needed if their perimeter security/intrusion detection system was not in service, administrators' (from 30 institutions) answers ranged from a low of 1 to a high of 24 additional personnel (with an average of 5). Their estimated additional annual cost for these staff members averaged $224,342 (range from a low of $40,000 to a high of $648,000).

Environmental Factors

Perimeter security systems exist in an environment containing a number of detrimental conditions. The greatest environmental problems for the responding institutions were lightning, wind, and hail. Table 1-16 shows the environmental factors respondents identified as causing the greatest problems.

Other factors that had less effect on perimeter security technology were extreme cold or heat, dust storms, earthquakes, standing water, soil erosion, uneven terrain, water running through buried conduits, and vibrations caused by traffic. Underground utilities had no effect on any system, but problems had been reported because of animals, birds, fog, and basketballs on recreation decks.

Table 1-16
Detrimental Environmental Factors

	No. of Facilities	%* Affected
Lightning	14	38
Wind	13	33
Hail	11	30
Power Surges	11	28
Snow/Ice	10	27
Debris	8	21
Rain	7	18

* The total percentage exceeds 100 because a number of institutions reported more than one kind of detrimental environmental factor.

* Only ten respondents provided information on both the length of their perimeter and the number of nuisance alarms. The relationship between these two factors (rho = 0.22) was small and statistically insignificant.

Several examples of environmental factors that nullified security systems were mentioned by respondents. In one, microwave sensors installed at a truck sally-port were struck by lightning causing the fuses to open. At a facility that had taut wire technology, heavy snows kept the system in a state of constant alarm.

SYSTEM SATISFACTION

Almost all (91 percent) of the respondents thought their current perimeter systems were appropriate for their facilities' security levels; the rest believed that the security levels of their institutions demanded additional or newer systems.

Most administrators agreed that their perimeter security/intrusion detection systems were sufficiently comprehensive. Eighty-two percent believed that leaving out any part of their technology would impair its operation.

Respondents at half the facilities had no requests for additional equipment; the remainder-whether or not they believed that their current security systems met the needs of their facilities' security levels-had some other technology on their wish lists, either to replace or to enhance the current systems. For example, 27 percent wanted motion detectors for better visibility and faster reaction, while 20 percent wanted video cameras for the same reasons. One facility wanted to change all hard-wire to a fiber-optics system and thereby eliminate electrical interferences.

Also deemed desirable by some administrators were:

- Alarms that respond directly to perimeter patrol vehicles to cut response time,
- An electronic detection system that could replace tower guards, and
- Vehicular patrols with zone-detection readouts.

The current perimeter security equipment in 77 percent of the sampled facilities was chosen to meet specific needs, including increased reliability, enhanced perimeter security, and total coverage. In 95 percent of the cases, this technology solved the problem to the satisfaction of the institutions' administrators. In the other 5 percent, problems continued, as reflected in too many false alarms or because of the need for additional video cameras.

Conclusions and Issues

CONCLUSIONS

The perimeter security systems currently onsite in correctional facilities seem to be meeting expectations and causing a minimal number of problems. Nevertheless, the survey data revealed a number of areas of concern.

Environmental factors (such as lightning, wind, and hail) that cause nuisance alarms had the greatest detrimental effect. Lightning might have also contributed to instances of power surges, which were reported by 66 percent of the respondents.

Seven out of ten institutions (71 percent) that reported nuisance alarms from lightning and power surges had fence-mounted motion sensors. These were connected by electric cables and, therefore, might be more susceptible to this type of interference. Half of these facilities also used microwave systems, which were less susceptible.

Redundancy, in general, was a common, effective solution to weaknesses in the various technology systems. For instance, 88 percent of the facilities with microwave systems backed them up with video cameras. Microwave-equipped facilities that experienced dead zones in their perimeter security, added more razor wire and/or more officer coverage to remedy the problem.

However, redundancy was usually not part of resolving false alarm problems. When asked if redundant systems were chosen because they were susceptible to different types of false alarms, only 21 percent answered "yes."

Most false alarms were of the nuisance type, that is caused by environmental factors. Equipment was at fault only 15 percent of the time, and installation malfunctions only 7 percent of the time.

If administrators had more say in designing their perimeter security systems, would the number of nuisance alarms caused by environmental factors be reduced? Clearly, people onsite were more aware of, and more realistic about, the environmental factors that needed to be taken into consideration, than were headquarters staff. Headquarters staff, on the other hand, were more appreciative of the budgetary constraints than were the onsite staff.

Although most responding facilities had a daily routine for ***testing their*** technology, routine maintenance of system components was rare-possibly a result of the systems seldom requiring major repairs (only 16 percent of the facilities reported problems relating to installation or equipment). But zones failed with some regularity.

ISSUES

Ideally, before any decisions are made about perimeter security systems, correctional administrators should familiarize themselves with the advantages and disadvantages of each option and apply these considerations to the particular factors that must be taken into account at their own sites. Each factor should be weighed in light of the demands it makes on staff time and its relative importance in maintaining security. Only after there is a clear understanding of what each system has to offer ***to a given facility*** should the choice of perimeter technology be made.

One of the factors to be considered is ease of maintenance. The new technology must be compared with the maintenance demands of the in-place system. That is best done by establishing a routine, written maintenance schedule. Routine preventive maintenance will warn of problems early enough to secure parts and make adjustments ***before*** the zone or the system becomes inoperable. Also, a written log will establish the criteria against which to measure the technology to be purchased.

Any plan for preventing problems will, ideally, include programs that not only maintain equipment, but also train staff in obtaining operating skills. Scheduled training, including refresher courses, and regular equipment checks will help keep all perimeter zones functioning.

Survey respondents were eager for others to learn from the problems they had experienced. They provided a list of issues to think about in evaluating your own perimeter security system:

1. Determine precisely what the hazards are to the facility's perimeter.

2. Consider relevant environmental factors when planning for a new (or upgraded) perimeter system.

3. Determine which perimeter technology is least susceptible to the particular environmental factors present at your facility.

4. Contact other users of the equipment to be purchased to learn where the weaknesses in each system are.

5. Include in the planning process considerations regarding redundancy so that weak points in one system will be covered by another technology. Ensure that the systems being installed are integrated with existing ones.

6. Determine whether the facility has the appropriate electrical wiring for the system (or systems) being considered.

7. Examine the size of the perimeter security zones. (Smaller is better--easier to localize alarms, speed-up response, and minimize interruption of the facility's operations.)

8. Purchase equipment for which parts are readily available, and will remain available, once the system is installed, and for which there are local contractors who can provide 24-hour service.

9. Determine whether or not the system has a good warranty-one that is explicit as to what is covered.

10. Consider whether or not the system will meet the facility's projected needs for the next 5 years.

11. Check plans for perimeter security system installation prior to initiation.

12. Have a trained staff member monitor installation to ensure that the installers are properly trained and working appropriately.

13. Plan to conduct defeat-testing of the system, post-installation, in situations that simulate actual operations.

14. Ensure that the installer, vendor, and/or manufacturer is under a performance bond. Determine how the bond will be enforced in the event there are problems with the system.

15. Have the vendor provide detailed drawings of the system after it is in place, to simplify maintenance and repair.

16. Obtain schedules for maintenance and repair from the manufacturer, vendor, and/or installer, and a schedule for (and information on) appropriate testing methods.

17. Determine whether or not maintenance and repair of the system will be accomplished by facility staff or by a maintenance contract.

18. Plan for staff to be trained in how to operate, maintain, and repair the system. Try to arrange the training as part of the sales contract.

19. Plan how follow-on training will be provided for both present personnel and new hires.

20. Consider whether or not this system is necessary to answer the needs of the institution for perimeter security or whether it is a case of electronics for electronics' sake.

Chapter 1

Questionnaire Data-Perimeter Security Systems

55 Responses

Fence-Mounted Motion Sensor	23	Infrared Sensors	8
Seismic Sensor In-Ground Cable	2	Ported Coaxial Cable	2
Taut Wire	14	Video Motion Detection	5
Microwave Sensors	25	Electric Field Sensors	4
Towers	31	Perimeter Patrols	38
Canine Patrols	4	Video Cameras	28
Other (specify)	13 (covered in text)		

1. Is the intrusion detection/perimeter security system appropriate for the current security level of the facility?
Yes 41 No 4 Don't Know 2 No Response 8

2. If no, what is the nature of the problem? (covered in text)

	Yes	No	No Response
3. Is there a wall around the perimeter?	10	41	4
4. Is/are there fence(s) around the perimeter?	50	2	3

5. If yes, how many fences are there?
# of Responses - 49 Average # of Fences - 1.76 High 3 Low 1

6. Is razor wire used as part of the facility's perimeter security?
Yes 47 No 5 No Response 3

7. If yes, how many coils of razor wire are there?
# of Responses - 45 Average # of Coils - 4.71 High 15 Low 1

8. Where are the coils of razor wire located? [Check (x) ALL that apply.]

Inside the Interior Fence	17
Between Fences	26
On Top of the Fence	46
Inside Wall	6
Other (specify)	10 (covered in text)

9. If the razor wire is on top of the fence, how is it attached? (covered in text)

10. How long is the perimeter?
# of Responses - 43 Average Length - 4711.67 feet High 18480 Low 100

11. Is the intrusion detection/perimeter security system zoned?
Yes 39   No 11   Don't Know 0   No Response 5

12. If yes, how many zones are there?
# of Responses - 37   Average # of Zones - 16.41   High 59   Low 1

13. How long is the longest zone?
# of Responses-   Average Length - 389.68 feet   High 900   Low loo

14. How long is the shortest zone?
# of Responses - 30   Average Length - 124.20 feet   High 800   Low 10

15. Would it be easy for inmates to determine where detection zones are?
Yes 27   No 14   Don't Know 3   No Response 11

16. What is the average number of seconds from detection to assessment?
# of Responses - 33   Average - 40.45 seconds   High 300   Low 1
Don't Know 6

17. How many seconds' delay does the barrier offer?
# of Responses - 15   Average - 35.73 seconds   High 300   Low 2
Don't Know 17

18. How does staff respond to an alarm? (covered in text)

19. How many towers are currently operated at the facility?
For 24 hours:
# of Responses - 27   Average # of Towers - 4.48   High 12   Low 1

For one shift but less than two:
# of Responses - 12   Average # of Towers - 1.67   High 4   Low 1

For two shifts but less than three:
# of Responses - 7   Average # of Towers - 3.29   High 9   Low 1

20. If you use perimeter patrols, which of the following are used? [Check (x) ALL that apply.]

Officer in Roving Vehicle	37
Officer in Stationary Vehicle	11
Mounted Officer	0
Officer on Foot	15
Canine Patrol	4
Other (specify)	7 (covered in text)

21. What type(s) of vehicle(s) is (are) used? [Check (x) ALL that apply.]

Sedan	11
Standard Pickup Truck	22
4-Wheel Drive	17
Other (specify)	13 (covered in text)

22. Perimeter patrols are [Check (x) ONE]:

Inside the Perimeter	11
Outside the Perimeter	42

23. Are the officers who patrol the perimeter armed?
Yes 34 No 11 Don't Know 0 No Response 10

24. If yes, the officers are quipped with [Check (x) ALL that apply]:

Sidearms	26
Shotguns	25
Rifles	6
Other (specify)	6 (covered in text)

25. If there is more than one type of intrusion detection/perimeter security system, were they installed at the same time?
Yes 21 No 18 Don't Know 1 No Response 15

26. If the systems were not installed at the same time, why was most recent one installed? (covered in text)

27. An alarm is declared when [Check (x) ONE]:

All Systems Go Into Alarm	1
One System Goes Into Alarm	35
Other (specify)	8 (covered in text)

	Yes	No	Don't Know	No Response
28. If more than one system must go into alarm to declare an alarm, were the systems chosen so they would be susceptible to different false alarms?	3	11	2	39
29. Does the facility conduct probability of defeat testing?	30	9	2	14

30. If yes, how many times will the system go into alarm in a typical 100 attempts?
# of Responses - 27 Average # of times - 98.96 High 100 Low 90
Don't Know 13

31. Does the facility test alarm response time? Yes 26 No 13 Don't Know 3 No Response 13

32. Are there dead zones in the perimeter security system (e.g., areas that are not covered by sensors)?
Yes 8 No 33 Don't Know 1 No Response 13

33. If yes, what has been done to cover the dead zones? (covered in text)

34. Is the system backed up by its own uninterrupted power system?
Yes 39 No 3 Don't Know 0 No Response 13

35. If yes, for how long can the emergency power system operate the perimeter security system?
# of Responses - 17 Average - 107.65 hours High 1000 Low 2
Don't Know 4

36. If the intrusion detection system were not in service, how many additional officers (based on an 8-hour shift) would be required to ensure perimeter security on a 24-hour basis?
# of Responses - 30 Average # of Officers - 5.37 High 24 Low 1
Don't Know 7

37. Including fringe benefits, what would be the yearly cost of staffing these additional posts?
# of Responses - 23 Average - $224,342.17 High $648,000 Low $40,000
Don't Know 12

	Yes	No	Don't Know
38. Does the intrusion detection system use a control panel/ console with a status indicator?	36	4	0
39. If yes, is the indicator reliable?	34	0	0
40. Is the alarm information that is received easy to read?	37	0	0

41. Where is the control panel located? (covered in text)

42. Are panels mounted in patrol vehicles?
Yes 9 No 31 Don't Know 0

43. If yes, how many patrol vehicles have panels?
# of Responses- Average # of Vehicles - 2.22 High 3 Low 2

44. The intrusion detection system is in use [Check (x) ONE]:

Always	39
Frequently	1
Often	0
Rarely	0
Never	0

45. Was the equipment installed according to the manufacturer's recommendations?
Yes 33 No 0 Don't Know 7

46. Did the facility experience bugs in the system after installation was complete?
Yes 27 No 9 Don't Know 4

47. If yes, for how long?

Don't Know 5

Days
# of Responses - 4
Average # of Days - 25.50
High 90

Months
# of Responses - 7
Average # of Months - 5.57
High 12

Weeks
# of Responses - 3
Average # of Weeks - 4
Low 2High 8Low 2

Years
# of Responses - 3
Average # of Years - 2
Low 2High 2Low 2

48. Were additional funds required to debug the system?
Yes 6 No 24 Don't Know 6

49. The specifications were written by [Check (x) ALL that apply]:

Facility	10
Consultant	17
Vendor	14
There were no specifications	2
other (specify)	10 (covered in text)

	Yes	No	Don't Know
50. Could any function or part of the system have been eliminated without impairing the operation?	6	28	5
51. Was a performance bond required of the supplier/ vendor/installer?	19	5	15
52. Was the supplier/vendor installer held to the performance bond?	18	5	14
53. Does this facility have an established training class in which staff learn to:			
a. Operate the perimeter security system?	13	23	
b. Maintain and repair the system?	14	23	

54. How many hours of training are required for staff to learn to:

a. Operate the perimeter security system?	b. Maintain and repair the system?
# of Responses - 25	# of Responses - 12
Average - 7.68	Average - 33.83
High 80 Low 1	High 100 Low 8

55. What percentage of staff members is trained to:

a. Operate the perimeter security system?	b. Maintain and repair the system?
# or Responses - 26	# of Responses - 22
Average - 26.15%	Average - 2.52%
High 80% Low 2%	High 10% Low .32%

56. The training is provided by (Check (x) ONE):

	Operate the System	Maintain the System
Vendor	8	9
Manufacturer	0	7
Facility	25	10
Other (specify) (covered in text)		

57. Who is responsible for maintenance and repair of the intrusion detection/perimeter security system? [Check (x) ALL that apply.]

Staff	26
Manufacturer	9
Outside Contractor	23
Other (specify)	3 (covered in text)

58. If staff, which staff are trained to maintain and repair the system? [Check (x) ALL that apply.]

Line Officers	0
Technicians	25
Other (specify)	7 (covered in text)

59. What is the average amount of down-time for:

Repairs

Hours
# of Responses - 14
Average - 14.29 Hours
High 120 Low 1

Days
# of Responses - 3
Average - 2 Days
High 3 Low 1

Weeks
# of Responses - 2
Average - 4 Weeks
High 6 Low 2

Months
# of Responses - 0
Average - 0
High 0 Low 0

Unscheduled Maintenance

Hours
# of Responses - 14
Average - 6.79 Hours
High 24 Low 1

Days
# of Responses - 2
Average - 1.50 Days
High 2 Low 1

Weeks
# of Responses - 2
Average - 1.5 Weeks
High 2 Low 1

Months
# of Responses - 1
Average - 1 Month
High 1 Low 1

60. If staff now performs maintenance/repairs, do you believe a maintenance contract would be an improvement?

a. For Cost	Yes 3	No 22	Don't Know 4	No Response 3
b. For Quality of Repairs	Yes 7	No 17	Don't Know 4	No Response 3

61. Does this facility stock spare parts for key components of the perimeter system? Yes 24 No 14

62. Are replacement parts readily available from the factory or dealer? Yes 34 No 3

63. What is the average amount of time between breakdowns?
Don't Know 12

Hours
# of Responses - 2
Average - 14 Hours
High 24 Low 4

Days
# of Responses - 4
Average - 13 Days
High 30 Low 1

Weeks
# of Responses - 2
Average - 4 Weeks
High 4 Low 4

Months
# of Responses-ll
Average - 6.36 Months
High 12 Low 1

64. How often is maintenance/testing performed on the perimeter security system and what does it involve? [Check (x) ALL that apply.] (descriptions covered in text)

weekly	12
Monthly	7
Quarterly	2
Semiannually	3
Annually	3
Randomly	5
Other (specify)	17

65. Who performs the scheduled maintenance/testing and what are they responsible for? [Check (x) ALL that apply.] (descriptions covered in text)

Staff	30
Vendor	6
Outside Contractor	5
Other (specify)	3

66. If the facility has a scheduled maintenance/testing program, are there many problems that require repairs?
Yes 6 No 26 Don’t Know 3

67. What are the most common repairs that are required? (covered in text)

68. Have you had a zone down for more than 24 hours?
Yes 24 No 14 Don’t Know 0 No Response 17

69. If yes, for how long?

Hours
# of Responses - 0
Average - 0 Hours
High 0 Low 0

Days
# of Responses - 14
Average - 3.36 Days
High 10 Low 2

\ Weeks
# of Responses - 8
Average - 2.63 Weeks
High 6 Low 1

70. Why was the zone down? (covered in text)

71. How often during the past year was one or more zones down?
# of Responses - 26 Average # of Times - 9.88 High 50 Low 1

72. Does the facility experience false alarms (alarms caused by system malfunctions)?
Yes 13 No 24 Don’t Know 1 No Response 17

73. If yes, how often?

# of Times Per Day
# of Responses - 2
Average Times Per Day - 12.50
High 20 Low 5

# of Times Per Week
# of Responses - 4
Average Times Per Week - 3.25
High 5 Low 2

# of Times Per Month
# of Responses - 0
Average Times Per Month - 0
High 0 Low 0

# of Times Per Year
# of Responses - 4
Average Times Per Year - 15.75
High 50 Low 3

74. False alarms are typically due to [Check (x) ALL that apply]:

Installation Problems	4
Equipment Problems	8
other (specify)	5 (covered in text)

75. Does the facility experience nuisance alarms (e.g., alarms resulting from natural causes such as weather or animals)?
Yes 37 No 2 Don’t Know 0 No Response 16

76. Is there an established acceptable standard for maximum number of nuisance alarms?
Yes 14 No 23 Don’t Know 2 No Response 0

77. If yes, what is it?

# of Times Per Day
# of Responses-
Average Times Per Day - 4.88
High 12 Low 2

# of Times Per Week
# of Responses - 2
Average Times Per Week - 3
High 4 Low 2

# of Times Per Month
# of Responses-0
Average Times Per Month - 0
High 0 Low 0

# of Times Per Year
# of Responses - 1
Average Times Per Year - 48
High 48 Low 48

Don’t Know 2
Other (specify) 2 (covered in text)

78. How was the standard established? [Check (x) ONE.]

Staff’s Ability to Respond	7
Don’t Know	3
Other (specify)	6 (covered in text)

79. How frequent are nuisance alarms?

# of Times Per Day
# of Responses - 17
Average Times Per Day - 8.88
High 30 Low 2

# of Times Per Week
# of Responses - 6
average Times Per Week - 2.83
High 4 Low 2

# of Times Per Month
# of Responses - 4
Average Times Per Month - 76
High 250 Low 2

# of Times Per Year
# of Responses - 0
Average Times Per Year - 0
High 0 Low 0

Don’t Know 2
Other (specify) 7 (covered in text)

80. What is the method of assessing the cause of an alarm? [Check (x) ALL that apply.]

Audio	10
Video	13
Tower	13
Patrol Car	27
Other (specify)	12 (covered in text)

81. How much is the intrusion detection/perimeter security system affected by each of the following environmental factors? [For "a" through "r" place an (x) in the appropriate column.]

	Affected	Somewhat Affected	Not Affected	Don't Know	No Response
a. Rain	7	19	14	1	14
b. Wind	13	19	8	1	14
c. Snow/Ice	10	17	10	4	14
d. Lightning	14	14	9	3	15
e. Debris	8	15	15	2	15
f. Extreme Heat	3	7	26	4	15
g. Extreme Cold	5	8	24	4	14
h. Standing Water	3	5	30	2	15
i. Soil Erosion	3	4	29	4	15
j. Uneven Terrain	4	1	31	4	15
k. Traffic Vibration	2	1	34	3	15
1. Power Surges	11	15	13	1	15
m. Underground utilities	0	0	37	3	15
n. Water Running Through Buried Pipes	1	3	33	3	15
0. Hail	11	19	7	3	15
p. Dust Storms	2	6	19	13	15
q. Earthquakes	4	2	15	18	16
r. Other (specify)	7	4	0	1	43

82. How does staff respond to nuisance alarms? (covered in text)

83. Have you ever had an intrusion detection/perimeter security system that never worked?
Yes 4 No 34 Don't Know 1 No Response 16

84. If yes, what type system was it? (covered in text)

85. What was the nature of the problem? (covered in text)

86. Has your facility experienced escape attempts involving a breach of the perimeter since your present perimeter security system was installed?
Yes 18 No 22 Don't Know 0 No Response 15

87. If yes, how many attempts have been made?
# of Responses - 17 Average # of Attempts - 2.47 High 12 Low 1

88. How many were successful?
# of Responses - 12 Average # of Successful Attempts - 2.25 High 10 Low 1

89. Did the system alert staff of the attempts?
Yes 15 No 3 Don't Know 0 No Response 37

90. Is there any other detection system you would like to see used in your facility?
Yes 14 No 14 Don't Know 8 No Response 19

91. If yes, what kind? (covered in text)

92. Why? (covered in text)

93. Was this facility's perimeter security equipment chosen for a particular reason or to solve a particular problem or problems?
Yes 20 No 6 Don't Know 14 No Response 15

94. If the equipment was chosen for a specific reason, what was that reason? (covered in text)

95. Has the equipment met expectations in terms of solving the problem?
Yes 18 No 1 Don't Know 2

96. If it has not solved the problem, why? (covered in text)

Chapter 2

Locks and Locking Systems in Correctional Facilities

Abstract

Correctional Technology: A User's ***Guide*** is the product of a nationwide assessment of the experience correctional administrators have had with various types of technological systems. The purpose of this guide is to provide correctional administrators with a user-friendly source of information to aid planning and decisionmaking.

For this chapter on locks and locking systems, survey questionnaires were prepared, reviewed by corrections locking system experts, pilot-tested onsite, and revised in light of that input. The final version was sent to 48 correctional institutions selected to represent all areas of the country and all levels of security. Presurvey letters and follow-up telephone calls resulted in an 88 percent response rate.

The survey found four major locking systems were used by the responding facilities: manual, mechanical, electro-mechanical, and electric-pneumatic. Manual locks were used most frequently (95 percent of the sampled facilities).

The survey results indicated that there was a lack of standardization across control panel systems that could cause severe security problems. For example, a red control panel light could mean that a door is open, locked, or closed but not locked.

Most administrators who responded to this survey seemed confident their locking systems were doing what they were installed to do, and they reported few problems.

Table of Contents

LIST OF TABLES

Executive Summary

This survey on locks and locking systems resulted in an 88 percent response rate: 42 of the 48 facilities that were sent questionnaires responded. Forty percent of the responding facilities were opened since 1980, and another 40 percent were opened between 1940 and 1979. Large, medium, and small facilities were evenly distributed: 35 percent had an average daily population (ADP) of under 500 inmates, while another 35 percent had an ADP of 1,000 or more. Fifty percent of the maximum security facilities were clustered in the Midwest.

The survey data indicated, in the main, that four general approaches to locking systems were used by the responding institutions:

- Manual-human-power used to pull a lever or turn a wheel;
- Mechanical-involves a mechanism that requires only turning a key or throwing a bolt to make it perform;
- Electra-mechanical-the use of electric motors coupled with a mechanical release mechanism; and
- Electric-pneumatic-the use of pneumatic power for door movement or unlocking and electric power for activation.

Manual locks were used by most of the facilities (95 percent). Some institutions used more than one type of lock; 86 percent used key operated case locks and 29 percent had padlocks. In an overwhelming number of facilities, door hinges (93 percent), door closers (82 percent), and security screws (90 percent) were at the same security level as the lock.

Renovations or additions resulted in locking system changes in more than half (55 percent) the facilities reporting. Of these, 36 percent required new locks because additions to the facility were made, 28 percent changed locks when the institution's security level changed, while 16 percent had upgraded their locking systems.

In 42 percent of the cases, the new equipment involved remote control requiring the use of control consoles or panels that showed the status of specific doors. The control panels were more likely to indicate when doors were closed (97 percent) or open (94 percent), rather than locked (61 percent). In fact, this study found a lack of standardization across control panel systems that could present severe security problems. For example, a red light on a control panel could indicate either that a door is open (in 71 percent of the facilities), a door is locked (32 percent), or a door is closed (28 percent); a green light could indicate that a door is closed (in 64 percent of the institutions), a door is locked (56 percent), or a door is open (21 percent).

Fewer than half the respondents had a system to prevent the accidental release of a door.

Three-quarters of the facilities reported having locking systems that were tamper-resistant when installed, 49 percent had experienced incidents of tampering. The frequency of such efforts ranged from an average of twice a day to five times a month.

In almost three out of four facilities (73 percent), the locking system had never been damaged to the point that it was totally disabled. The average amount of down-time for locking systems per year was 121 hours. Ninety-two percent of the institutions reported having an emergency generator to ensure that power for their locking systems remained uninterrupted. The generators were designed to come on-line in less than a minute (39 seconds) from the onset of a power outage.

Most administrators seemed confident that their locking systems were doing the job they were installed to do, and problems with the systems appeared to be minimal. The most common reason for repairs was maintenance rather than equipment failures.

Staff in three-quarters of the sample institutions were trained to help the person primarily responsible for maintaining locks. On average, 7 percent of the staff at each facility received locking system training; usually this included the locksmith (65 percent).

Scheduled maintenance did not prevent the need for certain kinds of repairs, For example, lubrication was mentioned by 74 percent of the respondents as commonly needed maintenance. Environmental conditions also contributed to systems wearing down; dust, ice, humidity, and snow negatively affected from 21 to 26 percent of the systems.

Maintenance and testing were, in most cases (35 percent), the responsibility of the security officer, who did testing (59 percent), visual checks (35 percent), and maintenance (6 percent). The locksmith was responsible for maintenance and testing for 25 percent of the responding facilities, performing testing (50 percent), maintenance (33 percent), visual checks (17 percent), or repairs as needed. Most facilities (85 percent) stocked spare parts for important locking system components, although 68 percent found spare parts readily available.

More than half the respondents reported satisfaction with their locking systems, but the other 44 percent believed other systems would be better than the ones they had. Their wish list included the following:

- An interlocking system to enhance security and reduce staff error,
- A uniform system for better organization and key control,
- Computerization to make institutions more secure, and
- Positive locking devices to replace current friction devices to keep doors locked when they were supposed to be.

In general, the correctional facility locking systems currently in use seemed to be both appropriate and efficient.

Introduction

The lock is a symbol for corrections. The dictionary defines a lock as "a device used to provide restraint," a definition that also applies to a correctional institution. It follows, then, that in a correctional facility, locks and locking systems have a peculiarly urgent importance. Locks, and the systems of which they are components, must not only keep designated people in specified areas and unauthorized people out, but they also must control movement between areas.

The technology of locking systems has evolved steadily and significantly. As new facilities were built and older ones renovated or retrofitted, more efficient locking systems were installed. The newer devices, which can be controlled from a distance, not only better protect staff, but also lessen staff and inmate transit time.

In the discussion of the technology of locks and locking systems, the following definitions will be used:

- ***The*** term "locks" refers to a ***single*** lock on a single door. It is opened manually; i.e., a key is turned or a bolt is slid. An officer walks up to each door and unlocks the lock; the inmate comes out/goes in; then, the door is closed and the officer re-locks it. Whether the door swings in or out, or is on rollers, the procedure is the same.

- The term "locking systems" refers to a ***group*** of doors, each of which has a lock that may be unlocked and/or locked remotely. Typically, locking systems comprise a group of sliding doors, some or all of which are opened or closed at the same time.

Of the 48 institutions sent survey forms relating to locks and locking systems, 42 completed and returned them, producing an 88 percent response rate. The sampled facilities represent a wide range of correctional institutions in terms of their location, size, and age.

The objective of this chapter is to provide corrections administrators with information relevant to decisionmaking about locks and locking systems technology. It includes the following:

- A description, in nontechnical terms, of the types of technology in use;
- An indication of support systems and staff needed to install, operate, and service the various systems;
- Factors to be considered during the selection and planning for the use of technology; and
- Conditions under which particular technologies may be appropriate, reliable, effective, or efficient.

This chapter contains the following:

- An overview of locks and locking systems,
- A description of the characteristics of the institutions sampled in the survey,
- An analysis of the survey findings,
- Conclusions drawn from survey results, and
- Issues to consider when evaluating locks and locking systems.

Locks and Locking Systems: An Overview

There are almost as many different types of locking systems as there are correctional facilities. A locking system functions to lock and unlock doors; it allows doors to swing-or slide-open or shut. There are four general approaches to locking systems: manual, mechanical, electro-mechanical, and electric-pneumatic.

LOCKS

Manual locking devices are methods used to keep doors locked. They require an individual-typically a correctional officer-to manipulate the device every time each door is opened.

Deadbolts do not have keys. They are hand-operated at the door by sliding a bolt into or out of a secure fastener. Bolts are difficult to breach. Some problems may occur because deadbolts cannot be operated or monitored remotely, and bolts may bind under pressure thereby making it difficult to open the door.

Padlocks are among the simplest of locking devices. Each lock has its own key. Doors are locked and unlocked by hand. Problems with this type device include no remote operation, no mechanical override, and problems cannot be detected from a distance; additionally, keys may break or become lost.

Commercial lock sets are locked and unlocked by hand. They may use either individual or multiple keys and are difficult to pick. They can be monitored remotely and may be overridden at the door by a master key. Problems occur when keys break or are lost and when inmates block keyholes.

In honor dorms in some facilities, inmates are allowed to have room keys, but door locks can be overridden by the correctional officer's master key.

Detention locks are larger and stronger than padlocks or commercial sets. The keys are large enough to overcome bolt friction or warpage, and picking is difficult. Like lock sets, they may have multiple keys, but they are still locked and unlocked by hand at the door. These locks may be monitored from remote sites. Problems can occur because the officer must open and close locks repeatedly, and inmates may stuff keyholes.

There are two types of detention locks:

- ***Paracentric locks*** are the standard two-dimensional type with a configuration of pins and tumblers that is relatively easy to pick;
- ***Mortise*** or ***mogul loch*** are four-dimensional. The key has cuts on four sides and the lock has springs and ball bearings which intermesh with the key to both reduce wear and make the lock harder to pick.

LOCKING SYSTEMS

All locking systems combine mechanical linkages with some operating power.

Manual systems use human power to pull a lever or turn a wheel.

Mechanical systems involve a mechanism that requires only turning a key or throwing a bolt to make the device perform. Groups of doors can be operated (opened/closed) from a remote location by pulling a lever or turning a wheel that is connected to a device (such as a cable) that actually moves the doors. A potential problem is that one jammed door can jam all doors.

Electra-mechanical systems involve the use of electric motors coupled with a mechanical release mechanism. Electra-mechanical systems perform the same functions as mechanical systems; however, the device that causes doors to open or close is electrically activated by pressing a button. This type system may require locking at the door itself. It can be monitored and unlocked remotely; however, it can be overridden mechanically only at the door.

A potential problem is the failure of low-voltage solenoids to retract a bolt when the door is under pressure. (A solenoid consists of a coiled wire that, when electric current flows through it, sets up a magnetic field that creates mechanical movement.) If doors are designed to unlock automatically when there is a power failure, power outages may threaten security.

Electric-pneumatic systems use pneumatic (compressed air) power for door movement or unlocking and electric power for system activation. A potential problem is that doors cannot be opened from a remote location by mechanical means if the power is off. Clean, dry air, set at proper pressure levels, must be used for the system to function properly.

DOORS

Doors may either swing or slide to open and close.

Swinging doors can be operated either mechanically or electrically. For safety purposes doors should swing ***out*** from an inmate's cell or room. A door that swings into a cell or room can easily be blocked to prevent entrance or used to injure an officer unless it is equipped with a closer. Twenty-four percent of the respondents indicated they have doors that swing in.

Sliding doors have five functions: locking, unlocking, door movement open, door movement closed, and stop motion to avoid crushing someone against the door jamb. Because a door may be closed but not locked, an electric indicator panel with a colored light that signals when the sliding door is in an unlocked position is often used.

Sample Characteristics

A varied group of institutions responded to the locks and locking systems survey; 8 were in the Northeast, 13 in the South, 10 in the Midwest, 9 in the West, and 1 in Canada. Security levels were also well distributed: 12 minimum, 17 medium, 8 maximum (long-term, difficult inmates), and 4 mixed (i.e., no inmate group, in terms of security needs, exceeded two-thirds of the facility's population). Higher security facilities were in the Midwest.

Most facilities were relatively new; 40.5 percent were built since 1980 and another 40.5 percent between 1940 and 1979. Average daily population was evenly distributed, 35 percent averaged under 500 inmates, and another 35 percent had 1,000 or more.

LOCATION AND SECURITY LEVELS OF SAMPLE FACILITIES

Table 2-1 shows the distribution of 40 U.S. respondents. Most responding institutions were located in the South (32 percent). Table 2-2 shows the sample facilities' levels of security by percentage of respondents.

Table 2-1
Location of Sample Facilities

Location	n	%
Northeast	8	20
South	13	32
Midwest	10	25
West	9	23
Total*	40	100

* Excludes one Canadian facility that responded to this survey. There was also one nonresponse.

Table 2-2
Security Level of Sample Facilities

security Level	n	%
Minimum	11	27
Medium	17	43
Maximum	8	20
Mixed*	4	10
Total†	40	100

* Inmate population was less than two-thirds in any security category.
† Excludes one Canadian facility that responded to this survey. There was also one nonresponse.

Chi square analysis of the data used to develop Tables 2-1 and 2-2 reveals a nonsignificant statistical relationship between geographic location and security level of the facility.* There were more maximum security facilities in the Midwest than in any of the other regions.

AGE OF SAMPLE FACILITIES

All 42 respondents (including the one Canadian facility) provided the date when the institutions were opened (see Table 2-3). Seventeen of the facilities in the sample (40.5 percent) were built since 1980, and an additional 17 (40.5 percent) were opened between 1940 and 1979. Only three were opened before 1900.

Table 2-3
Date Facilities Opened

	n	%
Before 1900	3	7.0
1900-1939	5	12.0
1940-1979	17	40.5
1980-Present	17	40.5
Total	42	100.0

*χ^2 = 12.288; df=9; N.S. A similar, nonsignificant result was found if the mixed category was not included (X^2 = 10.693; df=6; N.S.).

POPULATION SIZE OF SAMPLE FACILITIES

Facility size by average daily population (ADP) is shown in Table 2-4. Table 2-5 breaks out the 40 U.S. respondents by region and ADP. Table 2-4 shows that the number of facilities that had an ADP under 500 equaled the number with an ADP of over 1,000 (35 percent each). Table 2-5 illustrates that the South, Midwest, and West each had an equal number of facilities with ADP under 500 (four each). In the South, these four facilities represented only 31 percent of that region's total respondents; whereas, four facilities equaled 44 percent of the sample of western respondents.

Table 2-4
Average Daily Population

Population	n	%
Under 500	14	35
500-999	12	30
1000+	14	35
Total*	40	100

* Excludes one Canadian facility that responded to this survey. There was also one nonresponse.

Table 2-5
ADP by Region

Population	Northeast	SOUTH	Midwest	West	Total
Under 500	2	4	4	4	14
500-999	2	5	2	3	12
1000+	4	4	4	2	14
Total*	8	13	10	9	40

• Excludes one Canadian facility that responded to this survey. There was also one nonresponse.

Chi square analysis of the data used to develop Tables 2-4 and 2-5 reveals a nonsignificant statistical relationship between ADP and location.*

* X^2 = 2.411; df=6; N.S.

Survey Findings

Given the relative newness of the facilities reporting, it was not surprising that seven out of ten (71 percent) had a locking system that was designed when the facility was constructed. Almost eight out of ten of these (78 percent) had locking systems installed as part of the security package.

Nevertheless, renovations or additions resulted in changes in more than half (55 percent) the facilities reporting. Of these, 36 percent required new locks because of additions to the facility, 28 percent more changed locks when the institution's security level changed, and 16 percent upgraded their systems.

LOCKS

Table 2-6 shows the percentage of use of different kinds of various locking devices. Manual locks topped the list at 95 percent. A number of institutions had more than one type of lock (which accounts for percentages not adding up to 100). For these, the oldest was usually manual (85 percent), and was slightly more likely to be paracentric than mogul. Another 25 percent of facilities had mechanical systems as their oldest, and a few (5 percent) had electric.

Manual locks were very common: 95 percent of the facilities reported having them. Some institutions had more than one type: 86 percent key operated case locks and 29 percent padlocks. Hardware was more likely to be par-acentric (60 percent) than mogul (48 percent).

Table 2-6
Locks - Usage

Type of Lock	No. of Facilities	%*
Manual	39	95
Electra-Mechanical	22	54
Mechanical	10	24
Electra-Pneumatic	3	7

• The total percentage exceeds 100 because a number of institutions reported having more than one kind of lock.

LOCKING SYSTEMS

Manual locking systems have not been made obsolete by technology, though some have been upgraded. The newer systems were electric (50 percent), manual (40 percent), and pneumatic (20 percent). Replacement was the sole reason for installing a new system in only 12 percent of facilities; expansion (42 percent) and upgrading (42 percent) were the most common explanations given. Seventy-four percent found their new systems more effective than their old systems.

DOORS

Table 2-7 shows that swinging doors accounted for 80 percent of all doors used, while power sliding doors were used by six out of ten facilities (58 percent). Most often these were chain-driven (73 percent), though rack-and-pinion drives were used frequently (45 percent).

Remote release locks were prevalent; nine out of ten facilities had them on at least some doors. These locks were more likely to be found on swinging doors (78 percent) than on sliding doors (38 percent). Electrical release was slightly more likely to be 110 volts (55 percent) than 24 volts (47 percent). But whether the voltage was high or low, all facilities with remote release locks had a mechanical override for use during power outages.

Administrators generally agreed that their locking systems were efficient, and appropriate to the current security level of the facility (83 percent). Eighty-five percent thought no part could be eliminated without impairing the operation of the entire system.

Facilities reported that door hinges (93 percent), door closers (82 percent), and security screws (90 percent) were at the same security level as the lock.

Table 2-7
Doors- Usage

Type of Door	No. of Facilities	%*
Swinging	33	80
Out of Cell/Room	24	73
Into Cell/Room	9	27
Sliding	22	58
Chain Drive	16	73
Rack-and-Pinion	10	45
Cable Drive	1	5
Hydraulic	1	5
Pneumatic	1	5

* The total percentage exceeds 100 because a number of institutions reported having more than one kind of door.

CONTROL PANELS

Thirty-eight institutions used control rooms to manage their locking systems. The average number of these per facility was 5, with a high of 19 and a low of 1. An average of 9 remote control panels were used in 38 of the sampled institutions. The range in number of control panels used by the institutions was wide-from a high of 79 to a low of 1. Twenty-six facilities had work stations, with the average number being 14, and ranging from a high of 65 to a low of 1.

Control consoles, whether in panels or in dedicated rooms, usually (83 percent) had door status indicators; 74 percent of the facilities considered these indicators reliable. Problems experienced by the remaining 26 percent included bulbs burning out, the need to constantly adjust door position switches, tampering by inmates who shorted-out the system by putting razor blades in the locks, and problems with status indicators.

Control indicators were more likely to show when doors were closed (97 percent) and open (94 percent), rather than locked (61 percent). A lack of standardization across systems was reported. For example, a red light could indicate that a door was open (71 percent), locked (32 percent), or closed (28 percent); a green light could indicate that a door was closed (64 percent), locked (56 percent), or open (21 percent).

Other panel signals of a door's status included a printout and a light (4 percent) or an alarm and flashing light (4 percent) for ***open*** doors, a printout (4 percent) for ***closed*** doors, and an amber light (6 percent) or a printout (6 percent) for ***locked*** doors. More than three out of four

(76 percent) of the facilities reported having disable switches or deadlock indicators on their control panels.

Fewer than half the respondents (46 percent) had a system to prevent an accidental release of a door. Such devices included the following:

- Separate select, release, and cancel buttons on the console that forced conscious control;
- An interlock on walk-through gates (sally-ports) so that only one door could be opened at a time;
- Switches covered with protective caps or located out of regular reach;
- A gang-release button cover that had to be lifted before groups of doors could be opened;
- Some of the cells in the segregation unit disconnected from the control panel and operated only by keys;
- Only manual-locking doors connected to the control panels; and
- A system of key control.

In every facility, the door control panels were secure from inmate access. Security was maintained in a variety of ways:

- The override feature could be operated only from central control.
- Controls were segregated either in an area secured by key-operated locks and staffed 24 hours a day, in a self-contained room with two security doors and armed officers both inside and outside, in a room accessed only through double-keyed doors, or in a room entered from outside the facility.
- Cell door controls were all manual, and the wing officer, who was off the tier, held the key to the panel.

PROBLEM AREAS

Tampering

Although 72 percent of the respondents reported that their locking systems were tamper-resistant when installed, 49 percent had experienced incidents of tampering. The frequency of such efforts ranged from an average of twice a day to five times a month; the majority (51 percent) reported that tampering attempts occurred randomly.

Administrators had tried to tamper-proof their original locking systems by adding security screws and rivets, installing electric locks that were tamper-resistant, checking locks daily, installing plates over bolts, modifying the inmate electric release buttons inside the cells to make the wiring inaccessible, and tightening supervision.

Power Outage

Survey replies indicated that 92 percent of the institutions had an emergency generator to ensure that power for locking systems remained uninterrupted; the other 8 percent used a battery-operated back-up power system. On average, emergency generators came on-line in less than a minute (39 seconds) after the commencement of a power outage; the range was from 2 seconds to 10 minutes. Power was maintained a minimum of 2 hours, with the average exceeding 2 days **(55** hours).

Few locking systems were computer-operated (13 percent); for those that were, half had memory support-batteries, and six out of ten had program backups. A failure in one area would rarely (6 percent) make the whole system inoperable.

Key Control

Housing unit staff and inmates had keys to individual cell or room doors in only 24 percent of the facilities. The priority accorded key control in responding facilities was very high. Every facility indicated that there was a record of every key and/or key ring in the institution. All facilities had a procedure for coping with lost keys:

- Lost keys were to be reported immediately;
- The facility was to be locked-down during the search for the lost keys; and
- If the keys were not found, the locks were to be rekeyed.

In addition, some institutions used chains and locks on the doors until the problem was solved. An inmate who lost his/her room or cell key was charged not only for the new key but also for repinning the lock.

One facility had a locking system that never worked. Its key access system was compromised because there were not enough staff to handle the administrative procedures for tracking the keys.

SYSTEM OPERATIONS

Specifications

Fifty percent of the time, a facility's locking system's specifications were stipulated by the central office (see Table 2-8). Others likely to be involved in the locking system design included the administrator (36 percent), a consultant (36 percent), a security officer (33 percent), a vendor (21 percent), or the facility locksmith (19 percent). Five percent of the facilities reported that there were no formal specifications. Almost three out of four (73 percent) of the institutions had the architect's as-built drawings to guide maintenance and repair staff.

Table 2-8
Specifications for Locking Systems

Written By:	No. of Facilities	%*
Central Office	21	50
Administrator	15	36
Consultant	15	36
Security Officer	14	33
Vendor	9	21
Facility Locksmith	8	19
No Specifications	2	5
Other	4	10

* The total percentage exceeds 100 because a number of institutions reported more than one source for locking systems specifications.

Bugs

There were bugs in the newly installed locking systems of seven out of ten facilities; in eight facilities the debugging process took at least a year-10 years in one case. At the other extreme, two institutions were able to solve their locking system problems in 2 to 5 days.

Only three out of ten facilities had to expend additional funds for debugging. Eighty-two percent of the respondents required a performance bond of the installer; 73 percent of these facilities required the bonded installer to fix any post-installation problems that developed with the locking system.

TRAINING

In 74 percent of the sample institutions, staff were trained to help the person primarily responsible for maintaining locks. However, this high percentage did not mean that large numbers of staff knew how to do repairs. Although one facility trained everyone, 37 respondents indicated that, on average, only 7 percent of staff were trained. These included the locksmith (65 percent), the security officer (40 percent), and electronics technicians (30 percent).

As shown in Table 2-9,52 percent of the facilities did their own lock system training. Some training was also presented by the vendor (33 percent), the manufacturer (24 percent), and the National Institute of Corrections (7 percent). Books and manuals as training devices got mixed reviews depending on the circumstances.

Table 2-9
Locking System Trainers

	No. of Facilities	%*
Facility	24	52
Vendor	14	33
Manufacturer	10	24
National Institute of Corrections	3	7
Other	5	12

* The total percentage exceeds 100 because a number of institutions reported more than one source for locking system trainers.

MAINTENANCE AND REPAIR

Maintaining locking systems in operating order was, primarily, the concern of facility staff (95 percent) as shown in Table 2-10. An outside contractor or the manufacturer was called in 10 percent and 7 percent of the time, respectively. Only three out of ten (31 percent) of the facilities had training classes to teach staff how to maintain and repair their systems.

Table 2-10
Locking System Maintenance

	No. of Facilities	%*
Facility Staff	40	95
Contractor	4	10
Manufacturer	3	7
Other	6	14

* The total percentage exceeds 100 because a number of institutions reported that work was conducted by more than one maintenance provider.

Schedule

Twenty-nine percent of the respondents checked their locking systems weekly; some performed full testing (58 percent) and others just visual checks. Another 21 percent scheduled monthly reviews; of these, 78 percent tested their systems, 22 percent did preventive maintenance, and 22 percent did visual checks. The greatest proportion of the respondents (33 percent) reviewed their systems quarterly; of these 93 percent did testing, 14 percent did maintenance, 14 percent visual checking, and 7 percent cleaned the system. Some (19 percent) checked the system semiannually, doing maintenance (75 percent), testing (38 percent), visual checks (25 percent), and cleaning (13 percent). There were also facilities (14 percent) that followed an annual schedule for maintenance (67 percent), testing (33 percent), and visual checks (17 percent).

A few facilities used other scheduling options. Six institutions did visual checks and testing daily, one inspected the locking system every shift, and one did maintenance only when time permitted or when something broke.

Facilities that had scheduled maintenance might still run into problems (46 percent). Lubrication was a common need (74 percent), and weather did its part to wear down systems (33 percent). Motors (24 percent) and bearings (17 percent) wore out and had to be replaced, as did pins and tumblers. There also were adjustments, repairs, and door alignment problems that resulted from normal use.

Functions

Maintenance and testing were most often (35 percent of the cases) the responsibility of the security officer. They tested the equipment in 59 percent of the facilities, did visual checks in 35 percent of the institutions, and maintained the equipment in 6 percent of the facilities. Locksmiths performed maintenance and testing for 25 percent of the responding facilities (see Table 2- 11).

Table 2-11
Type of Locks Maintenance

		Type of Maintenance (by % of No. of Responses - Each Type Personnel)			
Personnel	**No.***	**Visual**	**Test**	**Maintain**	**Total**
Security Officer	17	35	59	6	35
Locksmith	12	17	50	33	25
Technician	6	33	50	17	13
Other	13	-	-	-	27
Total	48				100

* **The total number exceeds the number of facilities in the sample because several facilities indicated that locks maintenance** was **performed by more than one kind of personnel.**

Others called on to test and maintain locking systems included fire safety specialists, an alternate locksmith, an assistant superintendent, training coordinators, regular maintenance staff, and key control officers. Generally, outside contractors were not used to maintain locking systems. Only one facility thought a contractor could repair locking systems more inexpensively than staff, but 25 percent thought the work might be done better by an outside contractor.

Down-Time

The majority of the respondents (21 facilities) averaged 121 hours per year of locking system down-time (range was from a low of 1 hour to a high of 2,000 hours per year).

Most facilities (85 percent) stocked spare parts for important locking system components. Although 68 percent found spare parts readily available, others cautioned: "It ***can take up to 3 weeks to obtain parts from the factory or dealer."***

Environmental Factors

In almost three out of four facilities (73 percent), the locking system had never been damaged to the point where it was totally disabled. However, weather and environmental factors (Table 2-12) had detrimental effects in 33 percent of the reporting institutions. Factors reported as definitely having a negative effect on locking systems included dust, ice, humidity, and snow. One facility had a unique problem: Bees built nests in the locks.

Table 2-12
Detrimental Environmental Factors
(% Affected)

	%
Dust	26
Ice	25
Humidity	21
Snow	21

Conclusions and Issues

CONCLUSIONS

More than half the respondents reported satisfaction with their locking systems; the other 44 percent believed other systems, such as the following, would be better than those they had:

- An interlocking system to enhance security and reduce staff error;
- A uniform system to provide better organization and key control;
- Computerization to make the institution more secure; and
- Positive locking devices (e.g., deadbolts) to replace the current friction devices to keep doors locked when they were supposed to be.

Facilities tended to install new locking systems to solve a particular problem (64 percent), such as the need for additional security or the need to replace an obsolete system. Ninety-six percent of the new systems resolved the problem; the one that did not was compromised because doors could be opened without visual confirmation.

ISSUES

Based on the information provided by the survey data, a number of issues emerged that administrators need to consider when locks and locking systems are being designed or upgraded:

1. Prepare a list, with input from staff, of the requirements the new system should meet now and in the next 5 to 10 years.

2. Purchase equipment for which parts are readily available, and will remain available, once the system is installed, and for which there are local contractors who can provide 24-hour service.

3. Determine whether or not the system has a good warranty, one that is explicit as to what is covered, and will not expire before the system is completely debugged.

4. Make sure the system's warranties cover not only the communications equipment, but also transmission lines and wiring.

5. Take into consideration environmental factors that may affect the system's operation.

6. Check decisions with colleagues in other institutions and systems to benefit from their experience (i.e., to learn where the weaknesses are in each system).

7. Check plans for locking system installations prior to initiation.

8. Ensure that hinges, locks, electronics, and doors are all of the same security level. Heavy security locks will not hold up on low security construction. The system (or systems) being installed should be integrated with existing ones.

9. Determine whether the facility has the appropriate electrical wiring for the system (or systems) being considered.

10. Have a trained staff member monitor installation to ensure that the installers are properly trained and working appropriately.

11. Conduct defeat-testing of system components in actual operations simulations.

12. Obtain schedules for maintenance and repair from the manufacturer, vendor, and/or installer, and a schedule for (and information on) appropriate testing methods.

13. Have the vendor provide detailed drawings of the system, after it is in place, to simplify maintenance and repair.

14. Have the manufacturer, rather than a contractor, provide a maintenance contract.

15. Ensure that the installer, vendor, and/or manufacturer is under a performance bond. Determine how the bond will be enforced in the event there are problems with the system.

16. Plan for staff to be trained in how to operate, maintain, and repair the system. Try to arrange the training as part of the sales contract.

17. Decide what staff should be trained and what follow-on training will be scheduled.

18. Consider whether or not this system is necessary to answer the needs of the institution or whether it is a case of upgrading for the sake of upgrading.

Chapter 2

Questionnaire Data-Locks and Locking Systems

42 Responses

		Yes	No	Don't Know
1.	The locking system was &signed when the facility was designed.	27	11	4
2.	The locking system was installed as an integral part of the total security package.	31	9	2
3.	Renovations/additions resulted in changes to the locking system of the facility.	22	18	0

4. Describe the changes (e.g., adding new locks/locking system or retrofit). (covered in text)

5. If the facility uses more than one type of locking system, list them in the order in which they were installed, the oldest first, the newest last. (covered in text)

6. Why was the most recent one installed (e.g., expansion, replacement, upgrade, etc.)? (covered in text)

7. The most recently installed locking system was installed [Check (x) ONE]:

To replace another system	20
In addition to other systems	17
Don't Know	0

8. Is the newest locking system more effective than the previous system?
Yes 23 No 8 Don't Know 1 No Response 10

9. The facility has mechanical locks.
Yes 39 No 2 Don't Know 0 No Response 1

10. Mechanical locks are [Check (x) ONE]:

Key-Operated (case locks)	36
Pad Locks	12

11. Standard hardware is [Check (x) ONE]:

Mogul	20
Paracentric	25

12. The facility has power slide doors. Yes 22 No 16 Don't Know 0

13. Power slide doors are [Check (x) ONE]:

Rack-and-Pinion	10
Pneumatic	1
Chain Drive	16
Cable Drive	1
Hydraulic	1

	Yes	No	Don't Know	No Response
14. The facility has remote release locks.	36	4	0	2
15. Doors with remote release locks swing.	31	8	0	2

16. The cell/room doors swing [Check (x) ONE]:

Into cells/rooms	9
Out of cells/rooms	24

17. Doors with remote release locks slide.
Yes 14 No 23 Don't Know 0 No Response 5

18. Electrical remote release is [Check (x) ONE]:

High Voltage (110 volts)	23
Low Voltage (24 volts)	20

	Yes	No	Don't Know	No Response
19. The remote release locks have a mechanical override.	37	0	1	4
20. Could any function or part of the locking system have been eliminated without impairing the operation?	5	28	5	4
21. The locks and locking system are appropriate for the current security level of the facility.	35	7	0	0
22. The door hinges are the same security level as the lock.	37	3	**2**	**0**
23. The door closures are the same security level as the lock.	32	7	**2**	**1**

24. The security screws are the same security level

Yes 36	No 4	Don't Know 2	No Response 0

25. The facility has [Check (x) ALL that apply and indicate how many.]

Control Rooms	Remote-control Panels
# of Responses - 38	# of Responses - 32
Average # of Control Rooms - 5.26	Average # of Control Panels - 9.06
High 19 Low 1	High 79 Low 1

Work Stations	Rovers
# of Responses - 26	# of Responses - 24
Average # of Work Stations - 14.35	Average # of Rovers - 5.42
High 65 Low 1	High 50 Low 1

26. Do the control panel(s)/console(s). in control rooms and other locations have

Yes 33	No 7	Don't Know 0

27. If so, are the indicators reliable?

Yes 25	No 9	Don't Know 0

28. If no, what is the nature of the problem? (covered in text)

29. What modes are indicated by the control panel(s)/console(s)? [Check (x) ALL that apply.]

Open	31
Closed	32
Locked	20
Don't Know	0
Other (specify)	(covered in text)

30. How is each mode indicated on the control panel(s)/console(s) (e.g., different color lights)? (covered in text)

		Yes	No	Don't Know	No Response
31.	Is there a disable switch or deadlock?	28	9	1	4
32.	Is there a system to prevent accidental release of the doors?	16	19	3	4

33. If yes, what is it? (covered in text)

34. Are the controls secure from inmate access?

Yes 39	No 0	Don't Know 0	No Response 3

35. If yes, how is security maintained? (covered in text)

36. Was the locking system tamper-resistant as installed?

Yes 26	No 10	Don't Know 6	No Response 0

37. Has the facility experienced incidents of tampering?

Yes 19	No 20	Don't Know 2	No Response 1

38. Tampering typically occurs:

Times Per Day	Times Per Month
# of Responses - 1	# of Responses - 1
Average Times Per Day - 2	Average Times Per Month - 5
High 0 Low 0	High 0 Low 0
Randomly 18	

39. What has been done to the original design to make the system tamper-resistant? (covered in text)

40. The back-up uninterrupted power system is [Check (x) ONE]:

Battery-Operated	3
Emergency Generator	36
Don't Know	0
No Response	3

41. If it is an emergency generator, what is the time lapse for the generator to come on line?
# of Responses - 35 Average - 38.71 Seconds High 600 Low 2
Don't Know 0

42. For how long will the emergency generator operate the locking system?
# of Responses - 13 Average - 54.85 Hours High 169 Low 2
Don't Know 3

		Yes	No	Don't Know	No Response
43.	Is the locking system computer-operated?	5	35	0	2
44.	If yes, are there memory support batteries?	2	2	1	0
45.	Is there a program back-up?	3	2	0	0
46.	Would there be a failure of the entire system if one area went down randomly?	2	29	0	11
47.	Does the housing unit staff have keys to individual cell/room doors?	32	7	**0**	**2**
48.	Do the inmates have keys to their cell/room doors?	10	31	**0**	**1**
49.	If keys or key rings were lost, would the facility know which keys were lost and what they go to?	42	0	**0**	**0**
50.	Is there a policy or procedure for coping with lost keys?	41	0	**0**	**1**

51. If there is a policy, briefly describe it. (covered in text)

52. The specifications for the system were written by [Check (x) ALL that apply]:

Facility Locksmith	8
Security Officer	14
Administrator	15
Central Office or Headquarter Staff	21
Consultant	15
Vendor	9
There were no specifications.	2
Don't Know	8
Other (specify)	4 (covered in text)

53. Did the facility experience bugs in the locking system after it was completed?
Yes 21 No 9 Don't Know 8 No Response 4

54. If yes, for how long?

Don't Know 6

Days	Weeks
# of Responses - 2	# of Responses - 0
Average # of Days - 3.50	Average # of Weeks - 0
High 5 Low 2	High 0 Low 0

Months	Years
# of Responses - 7	# of Responses - 8
Average # of Months - 7.29	Average # of Years - 5.50
High 18 Low 1	High 10 Low 1

55. Has the system been successfully debugged?	Yes 20	No 7	Don't Know 2	No Response 13
56. Were additional funds required to debug the system?	Yes 7	No 16	Don't Know 6	No Response 13
57. Was a performance bond required of the supplier/vendor/installer?	Yes 14	No 3	Don't Know 17	No Response 8
58. Was the supplier/vendor/installer held to the performance bond?	Yes 8	No 3	Don't Know 20	No Response 11

59. Who is responsible for maintenance and repair of the locking system? [Check (x) ONE]

Staff	40
Manufacturer	3
Outside Contractor	4
0ther (specify)	6 (covered in text)

		Yes	No	Don't Know	No Response
60.	Does the facility have an established training class in which staff learn to maintain and repair the system?	13	29	0	0
61.	Did the architects/engineers provide as-built drawings of the system for use by the maintenance staff?	22	8	8	4
62.	Is there staff trained to assist the person who is primarily responsible for the locks and locking system?	31	9	0	2
63.	Is there training for any/ all new staff who will be working on the locks and locking system?	28	11	0	3

64. What percentage of the facility staff members are trained to maintain and repair the system?
# of Responses - 37 Average - 7.22 % High 100 Low 1 DK 0

65. How many hours of training are required for a staff member to learn to maintain and repair the system?
# of Responses - 23 Average - 99.74 Hours High 1000 Low 2 DK 2

66. Which staff are trained to maintain and repair the system? [Check (x) ALL that apply.]

Locksmith	26
Security Officer	16
Electronics Technicians	12
Other (specify)	6 (covered in text)

67. The training is provided by [Check (x) ALL that apply]:

Vendor	14
Manufacturer	10
Facility	22
National Institute of Corrections	3
other (specify)	5 (covered in text)

68. How often is scheduled maintenance/testing performed on the locks and locking system and what does it involve (e.g., weekly visual inspection, etc.)? [Check (x) ALL that apply.]

Weekly	12 - 29%
Monthly	9 - 21%
Quarterly	14 - 33%
Semiannually	8 - 19%
Annually	6 - 14%
Other (specify)	9 - 21%

69. Who performs the scheduled maintenance/testing and what are they responsible for (e.g., security officer-weekly visual, etc.)? [Check (x) ALL that apply.]

Locksmith	12 - 29%
Security officer	17-40%
Technician	6 - 14%
Vendor	2 - 5%
Manufacturer	1 - 2%
Outside Contractor	0
Other (specify)	10-24%

70. If the facility has scheduled maintenance/testing, are there many problems that require repairs?

Yes 17	No 20	Don't Know 2	No Response

71. What are the most common reasons repairs are required? [Check (x) ALL that apply.]

Lubrication	31 - 74%
Worn Bearings	7-17%
Replace Motors	10-24%
Maintenance for Weather	14 - 33%
Other (specify)	14 - 33%

72. What is the average amount of down time per year for repairs?

Hours
# of Responses - 21
Average - 121.19 Hours
High 2000 Low 1

Days
# of Responses - 4
Average - 6.25 Days
High 12 Low 2

Weeks
# of Responses - 3
Average - 2 Weeks
High 3 Low 1

Months
# of Responses - 2
Average - 9 Months
High 12 Low 6

	Yes	No	Don't Know	No Response
73. If staff now perform maintenance/repair, do you believe a maintenance contract would be an improvement?				
a. For Cost	2	32	3	15
b. For Quality of Repairs	8	27	2	5
74. Does the facility stock spare parts for key components of the system?	33	6	0	**3**
75. Are spare parts readily available from the factory or dealer?	26	12	2	**2**

76. Has the system ever been damaged to the extent that it became nonfunctional?
Yes 10 No 27 Don't Know 1 No Response 4

77. Please explain the circumstances. (covered in text)

78. To what extent is the locking system affected by each of the following environmental factors? [For "a" through "h" place an (x) in the appropriate column]

	Somewhat Affected	Affected	Not Affected	Don't Know	No Response
a. Humidity	8	12	18	2	2
b. Temperature	7	7	24	2	2
c. Rain	6	18	16	0	2
d. Dust	10	12	17	1	2
e. Lightning	5	5	24	6	2
f. Snow	8	13	18	1	2
g. Ice	10	13	17	0	2
h. Other (specify)	1	1	0	0	40

79. Is there a locking system you feel would be better suited for your facility?
Yes 12 No 15 Don't Know 11 No Response 4

80. If yes, what kind? (covered in text)

81. Why would this be better suited to your facility? (covered in text)

82. Has the facility ever had a locking system that was never successfully installed or that never worked for any reason?
Yes 3 No 33 Don't Know 3 No Response 3

83. If yes, what type of system was it? (covered in text)

84. What was the nature of the problem? (covered in text)

85. Was the most recently installed locking system in this facility installed for a particular reason or to solve a specific problem?
Yes 21 No 12 Don't Know 4 NoResponse 5

86. If the equipment was installed for a specific reason, what was the reason? (covered in text)

87. Has the locking system met expectations in terms of solving the problem?
Yes 22 No 1 Don't Know 1 No Response 18

88. If it did not solve the problem, why? (covered in text)

Chapter 3

Internal Detection Systems in Correctional Facilities

Abstract

Correctional Technology: A User's ***Guide*** is the product of a nationwide assessment of the experience correctional administrators have had with various types of technological systems. The purpose of this guide is to provide correctional administrators with a user-friendly source of information to aid planning and decisionmaking.

For this chapter on internal detection systems, survey questionnaires were prepared, reviewed by experts in the field of internal detection in corrections, pilot-tested onsite, and revised in light of that input. The final version was sent to 66 correctional institutions selected to represent all areas of the country and all levels of security. Presurvey letters and follow-up telephone calls resulted in an 85 percent response rate.

Virtually every institution used hand-held and walk-through detectors to aid in contraband control. Administrators believed that hand-held metal detectors were the most effective. They also viewed X-ray machines as essential to institution security. Twenty-nine facilities (52 percent) used drug-detection canine teams for contraband detection and for building searches. Eighteen (26 percent) of the responding institutions owned their own teams; the remainder borrowed dog teams as needed.

Administrators who responded to the survey were generally satisfied with the ability of their internal detection technology to reduce contraband traffic.

Table of Contents

LIST OF TABLES

Executive Summary

Contraband represents one of the major threats to the security of a correctional institution. Corrections administrators have chosen a variety of ways to detect contraband. The sampled institutions represented all areas of the country and all security and population size levels.

Survey data from 56 institutions (an 85 percent response rate) indicate that the number of different kinds of internal contraband detection systems used by one institution ranged from 1 to 4; the average was 3.1, but most facilities used 4. Virtually every institution (98 percent) used hand-held detectors, and 93 percent used walk-through detectors. X-ray machines and drug detection canines were used by more that 50 percent of the respondents.

Administrators who responded to the internal detection systems survey were satisfied with their technology's ability to reduce the movement of contraband within their institutions. One advantage cited was that personnel were available for other assignments when detection equipment and dogs were used to search people and parcels entering the facility. In addition, 15 percent of the respondents believed that their internal detection equipment produced a deterrent psychological effect.

HAND-HELD DETECTORS

Of the three internal detection technology devices used by responding facilities, hand-held metal detectors were ranked as most effective. The more secure and larger the facility, the more these detectors were used. Over three-quarters of the facilities considered hand-held detectors essential to security, because they decreased the probability of contraband being introduced into the facility, and they decreased the additional staff time that would be required to conduct searches.

These devices were viewed by institution personnel as both reliable and durable. Sixty-nine percent of the respondents regularly tested their detectors. Because of the low breakdown rate and the availability of spare parts from the factory or dealer, only 15 percent of institutions stocked spare parts.

WALK-THROUGH DETECTORS

Walk-through detectors had been used by the respondents an average of 8.2 years (ranging from a low of 2 to a high of 19 years). The average number of walk-through detectors per facility was 2.9 (the range was from 1 to 13 devices). As was true for hand-held detectors, all walk-through detectors were bought rather than leased.

These devices were used to search people, most often visitors. Respondents believed that their walk-through detectors did a good job of discovering metal objects. False alarms were usually caused by other nearby metal objects (e.g., metal doorjambs).

Staff at 87 percent of the facilities tested walk-through equipment daily. Twenty-five of the sample institutions indicated that the average time between breakdowns was 162 days.

X-RAY MACHINES

Administrators said that X-ray machines were essential to institution security; without them, 86 percent of the respondents believed contraband would be much more likely to enter their facility.

About three out of four institutions (74 percent) tested their X-ray machines regularly, most on the average of six times a week. Testing was usually done by staff (81 percent of the cases).

DRUG-DETECTION CANINES

Eighteen of the sample facilities had their own drug-detection canine teams; other institutions used outside dog handlers or borrowed teams as needed. The average number of teams per facility was three. German shepherds were the most popular breed (59 percent), with Labrador retrievers a distant second (28 percent), and bloodhounds still further back in the pack (21 percent).

Canine teams were most often used for building searches (90 percent), to detect concealed narcotics (86 percent), and to track evidence (48 percent). Some institutions (31 percent) used dogs as a perimeter security system to prevent escapes. Dogs were also used to accompany escorts on medical trips, to patrol visiting rooms, to track escaped inmates, to assist in crowd control, to subdue riots, to detect explosives, to provide grounds control, and to search cars.

Forty-eight percent of the sample institutions required special qualifications for canine handlers, and in 95 percent of the facilities the dogs had to meet certain certification requirements. In all cases, handlers were personally responsible for the care and feeding of their animals. Usually (69 percent) the dogs lived with the handler.

One in four of the institutions reported problems regarding the use of canine teams, including an insufficient number of dogs, transition to a new handler when the old handler was promoted, and veterinary fees.

Introduction

Correctional institutions must not only control the movement of people, but they must also prevent the introduction of contraband into the facility's environment. They use internal detection systems to help them with contraband control.

Simply put, contraband is anything an inmate is not permitted to bring in at the time of admission, is not issued to him/her, is not purchased in the facility's commissary, or is received without permission from outside sources. In addition, a permitted item or substance found to be in excess of policy-established limits is also considered contraband. Contraband can be divided into subcategories:

- Items that can be used to aid in an escape, such as metal-altering tools, maps, money, and perimeter breaching equipment;
- Weapons or materials from which weapons may be fashioned,
- Drugs or alcohol;
- Nuisance contraband, which includes excesses of materials issued by the facility, such as clothing or food.

Because contraband can cause direct threats to the security and safety of an institution, those in it, and the public, a high priority is placed on contraband control. The first step in controlling contraband is detection. Knowing that comprehensive efforts are being made to prevent the introduction of contraband into an institution gives staff a sense of personal security, thereby lowering stress and increasing efficiency.

The objective of this chapter is to provide corrections administrators with information relevant to decisionmaking about internal detection systems technology. It includes the following:

- A description, in nontechnical terms, of the types of technology in use;
- An indication of support systems and staff needed to install, operate, and service the various systems;
- Factors to be considered during the selection and planning for the use of technology; and
- Conditions under which particular technologies may be appropriate, reliable, effective, or efficient.

This chapter contains the following:

- An overview of internal detection systems,
- A description of the characteristics of the institutions sampled in the survey,
- An analysis of the survey findings,
- Conclusions drawn from survey results, and
- Issues to consider when evaluating an internal detection system.

Internal Detection Systems: An Overview

Internal detection systems provide staff with technology that enables them to control the introduction of contraband into their institution. The leading systems in use are hand-held detectors, walk-through detectors, X-ray machines, and drug-detection canines.

Hand-held metal detectors were used in virtually all (98 percent) of the sample institutions. These are battery-operated, portable devices that create an electromagnetic field by passing a low electrical current through a soft iron core wrapped with a solenoid. The electromagnetic field detects the presence of metal, and the magnetic attraction causes an alarm to sound or a visible signal to be triggered.

These devices precisely locate metal objects being carried by a person. They are also used when walk-through detectors are not practical (e.g., for a person in a wheelchair).

Walk-through metal detectors, used by 93 percent of the respondents, are electronically equipped archways that sound an alarm when the person walking through is carrying more than a preselected amount of metal. These devices work on the same electromagnetic principles as hand-held detectors. They are usually placed at the main entrances into the facility and are located inside an institution at entrances into and exits from areas containing likely contraband material (e.g., industries).

X-ray machines were found in 66 percent of the responding facilities. X-rays, electromagnetic waves that are shorter than ultra-violet rays, are produced by a Coolidge tube in which highly accelerated electrons are aimed at a tungsten filament heated to a high temperature.

The outstanding feature of X-rays is their ability to penetrate through most materials, including packages and solids. These machines are able to search for contraband inside closed boxes and letters.

Drug-detection canines, used in 52 percent of the sampled institutions, they are specially trained dogs that work with a handler, in teams, to locate concealed drugs and explosives.

Sample Characteristics

In 1992, a survey was sent to 66 correctional facilities concerning their use of internal detection systems. Fifty-six facilities replied, producing an 85 percent response rate.

LOCATION

Table 3-1 shows the distribution of the 53 U.S. institutions that responded. The distribution of the institutions across the country was fairly equal: 12 (23 percent) were in the Northeast, 15 (28 percent) in the South, 12 (23 percent) in the Midwest, and 14 (26 percent) in the West.

Table 3-1
Location of Sample Facilities

Location	n	%
Northeast	12	23
South	15	28
Midwest	12	23
West	14	26
Total*	53	100

* Excludes three additional Canadian facilities that responded to this survey.

SECURITY LEVELS

Table 3-2, which shows the facilities' security levels, indicates that medium security institutions had the highest representation (41 percent), while the remainder were fairly equally represented.

AGE OF SAMPLE FACILITIES

As shown in Table 3-3, most of the responding facilities were relatively new (80 percent had opened since 1939), and more than one-third of these (39 percent) were built since 1979.

POPULATION SIZE OF SAMPLE FACILITIES

The size of the sample institutions is shown in Table 3-4 as the average daily population (ADP); 46 percent had an ADP of 1,000 or more.

Table 3-2
Security Level of Sample Facilities

Security Level	n	%
Minimum	11	20
Medium	23	41
Maximum	10	18
Mixed*	12	21
Total	56	100

* Inmate population was less than two-thirds in any security category.

Table 3-3
Date Facilities Opened

	n	%
Before 1900	5	9
1900-1939	6	11
1940-1979	23	41
1980-Present	22	39
Total	56	100

Table 3-4
Average Daily Population

Population	n	%
Under 500	15	27
500-999	15	27
1000+	26	46
Total	56	100

Survey Findings

Corrections administrators generally chose to use more than one method of detecting contraband. The number of different systems used by one institution ranged from 1 to 4; the average was 3.1, but most institutions used 4. Table 3-5 shows the frequency of use (98 percent of the sample facilities -used hand-held detectors, and 93 percent used walk-through detectors). X-ray machines and drug-detection canines were used by more than 50 percent of the respondents.

Table 3-5
Internal Detection Systems - Usage

	No. of Facilities	%*
Hand-Held Detectors	55	98
Walk-Through Detectors	52	93
X-Ray Machines	37	66
Drug-Detection Canines	29	52

* The total percentage exceeds 100 because the institutions reported using more than one kind of internal detection system.

DEVICE EFFECTIVENESS

Respondents were asked to rank, in terms of effectiveness, the three internal detection technology devices: hand-held, walk-through, and X-ray detectors. A weighted score was calculated (see Table 3-6).* The results indicate that hand-held metal detectors were rated as most effective.

Table 3-5
Effectiveness in Contraband Detection

	Weighted Score	%*
Hand-Held Detectors	106	38
Walk-Through Detectors	99	35
X-Ray Machines	74	27
Total	279	100

* Percentage of total weighted score.

CONTRABAND DETECTED

Employing the same weighting system, replies were tabulated from the facilities regarding types of contraband they most frequently detected (see Table 3-7). Thirty-six percent of the respondents ranked drugs first, second, or third. Marijuana was the most frequently found contraband drug (44 percent).

The second most frequently discovered item was weapons, ranked first, second, or third by 26 percent of the sample institutions. Of all weapons found, prison-made knives, called shanks, topped the list.

* A point value of 3 was assigned for each first place rating, 2 points for second, and 1 point for third.

Respondents were asked about the number of shanks detected with and without the aid of detectors during the past year, and surprisingly, more were discovered ***without*** using technology. The averages per institution were 13.3 discovered with detectors and 33.8 without the use of detectors.

Table 3-7
Most Frequentfy Detected Contraband

	Weighted Score	%*
Drugs	**106**	**36**
Marijuana	47	44
Cocaine	22	21
Prescription	17	16
Valium, etc.	12	11
Hashish	6	6
LSD	2	2
Weapons	**76**	**26**
Nuisance Type	**40**	**13**
Home Brew	**33**	**11**
Unauthorized Items Brought in by Staff and/or Visitors	**22**	**7**
Money	**15**	**5**
Food	**5**	**2**
Total	**297**	**100**

* Percentage of total weighted score.

HAND-HELD DETECTORS

Table 3-8 shows the relationship between both security level and size of facility and the number of hand-held detectors. The more secure and larger the facility, the more these detectors were used.

The average number of hand-held detectors in a responding facility was 9 (ranging from 1 to 40). For 71 percent of the respondents, this number included spare units that could be used while others were being repaired or recharged.

Although hand-held detectors were used in virtually every institution (98 percent of the respondents), these devices varied considerably:

- 79 percent detected only metal objects,
- 69 percent had an automatic reset mechanism,
- 58 percent could not scan silently,
- 56 percent had a signal that was audible only,
- 44 percent had both visible and audible signals, and
- None had a signal that was visible only.

Table 3-8
Number of Hand-Held Detectors -
by Security Level and Size

Security Level	Average Number
Minimum	6
Medium	8
Maximum	12
Mixed	10
Size	
Under 500	4
500-999	8
1000+	11

Ninety-two percent of the respondents considered hand-held detectors reliable, and 87 percent rated them as being durable. Almost all respondents (98 percent) used hand-held detectors to search people (see Table 3-9). These individuals were inmates (89 percent), visitors (85 percent), vendors (64 percent), staff (51 percent), or simply anyone who could not pass through the walk-through detectors (5 percent).

Hand-held detectors were also used by the sample institutions to search the grounds (5 percent), recreation yards, or storage areas, and often to search objects like mattresses (69 percent), linens (51 percent), or packages (49 percent).

Seventy-seven percent of the facilities considered hand-held detectors essential to security, and said that without hand-held detectors, the probability of contraband being introduced into the facility would increase to 100 percent. Twenty-nine percent thought that the only alternative would be to use additional staff time to conduct searches.

Acquisition, Training, and Maintenance

None of the sample facilities leased hand-held detectors; everyone bought them. Where training was conducted, most often it was provided by the facility (63 percent), but occasionally by the manufacturer (17 percent) or the vendor (15 percent). Often (55 percent of the time) staff was responsible for maintaining and repairing these devices, though sometimes institutions called on the manufacturer (25 percent) or an outside contractor (25 percent).

Table 3-9
Searches Conducted With Hand-Held Detectore

	Weighted Score	%[*]
People[†]	54	98
Inmates	49	89
Visitors	47	85
Vendors	35	64
staff	28	51
Mattresses	38	69
Linens	28	51
Packages	27	49
Grounds	3	5
Other	3	5

[*] The total percentage exceeds 100 because a number of institutions reported that they conducted searches on more than one kind of entity.

[†] The breakdown of “People” exceeds its weighted score of 54 and the total percentage exceeds 100 because facilities indicated they search several different kinds of people.

There did not appear to be much concern with preventive maintenance. Only 29 percent of the reporting facilities had such a program, for a number of reasons. Very few (only five) institutions reported frequent breakdowns of their hand-held detectors; breakdown occurrences ranged from one a day to one a week, with the average every 3 days. At the other extreme, eight facilities averaged a breakdown of a hand-held detector only once every 5 months. Since almost all facilities had multiple hand-held detectors, breakdowns did not cause security problems. Moreover, because they were inexpensive, if one broke and could not be fixed, it was thrown away.

Only 15 percent of institutions stocked spare parts for their hand-held detectors; 77 percent reported that spare parts were readily available from the factory or dealer.

Testing

Hand-held detectors were tested regularly by 69 percent of the sample facilities. Twenty-five institutions reported they tested an average of 6 times a week (with a range from 1 to 21 times per week). Since this equipment was in daily use, any problems were detected immediately. Where hand-held detectors were tested, it was usually done by institution personnel (e.g., security staff or an electronics technician); an outside contractor was used by 13 percent of the reporting facilities. In institutions where staff performed maintenance, only 30 percent believed that a maintenance contract would decrease costs, and 36 percent thought the quality of repairs would improve with a maintenance contract.

Problems

Most of the time (88 percent), hand-held detectors met expectations. In the few instances where they did not, the problem had to do with either the presence or the absence of metal. Hand-held detectors did not work well when the target contraband was not metal, and they sometimes gave false alarms when there was too much metal nearby, such as metal doors or corridor grilles. For example, in one facility when hand-held detectors were passed below the subject's knee, they alarmed in response to the metal reinforcement rods in the building's floor.

WALK-THROUGH DETECTORS

Although one respondent had used walk-through detectors for only 6 months, the others had used them for an average of 8.2 years (ranging from a low of 2 to a high of 19 years). The average number of walk-through detectors per facility was 2.9 (with a range from 1 to 13 devices). As was true for hand-held detectors, all walk-through detectors were bought rather than leased.

Walk-through detectors were more likely than hand-held detectors to be considered an integral part of the institution's total security package (86 percent). Their absence, it was believed, would increase the likelihood of contraband entering the facility (82 percent) and require more staff time for searches (14 percent).

Location

In 56 percent of the reporting facilities, walk-though detectors were at all the entrances (see Table 3-10). Additional frequent placements were at the entrance to the visiting room (in 37 percent of the facilities), at the main entrance (21 percent), between cell houses (37 percent), and at the entrance to prison industries (29 percent).

Table 3-10
Location of Walk-Through Detectors

	No. of Facilities	%*
All Entrances	29	56
Visiting Room Entrances	19	37
Between Cell Houses	19	37
Industries Entrances	15	29
Main Entrances	11	21
Program/Work Areas	8	15
Vocational Education Area	5	10

* The total percentage exceeds 100 because a number of institutions reported that their walk-through detectors were located in more than one area.

uses

Walk-through detectors were used to search people, usually visitors (98 percent-see Table 3-11). Others searched were vendors (85 percent), inmates (75 percent), and staff (62 percent).

Though walk-through detectors discovered only certain metallic objects, they did their job well. In 87 percent of the reporting institutions, the detectors disclosed objects regardless of shape, position, or orientation, even if the person walked rapidly through the device. Almost all (94 percent) walk-through detectors automatically reset after an alarm.

Table 3-11
Subjects of Search Using
Walk-Through Detectors

	No. of Facilities	%*
Visitors	51	98
Vendors	44	85
Inmates	39	75
Staff	32	62
Other	4	8

* The total percentage exceeds 100 because a number of institutions reported that they search more than one kind of subject.

Table 3-12
Causes of Watk-Through Detector False Alarms

	Weighted Score	%*
Metal Nearby	29	28
Weather Related	26	25
Wind	6	23
Humidity	5	19
Rain	5	19
Cold	3	11.5
Heat	3	11.5
snow	2	8
Sun	2	8
Clothing	17	17
Power Surges	10	10
Touching/Bumping	9	9
Radio Waves	8	8
Static Electricity	3	3
Total	102	100

* Percentage of total weighted score.

Tampering

Most walk-through detectors (77 percent) were tamper-resistant when purchased, where they were not, three out of ten institutions modified them to make them so, usually by moving the devices' controls to a secured area (86 percent), or putting them under the constant observation of correctional officers (14 percent).

Problems

In 71 percent of the responding institutions, walk-through detectors were installed specifically to control contraband, for the most part (92 percent) they performed well.

False Alarms. Facilities ranked the three most frequent causes of false alarms with walk-through detectors. Table 3-12 was generated by using the same weighting procedure as used to rank device effectiveness (Table 3-6). The most common causes of false alarms were as follows:

- A metal object too close to the detector (28 percent);
- Atmospheric conditions (25 percent), such as wind, humidity, ram, cold, heat, snow, and sun; and
- Other sources, such as clothing (17 percent), power surges (10 percent), touching or bumping the unit (9 percent), radio waves (8 percent), static electricity (3 percent), and fluorescent lights and dust.

False alarms also resulted from equipment problems (78 percent) and installation difficulties (39 percent). For example, four facilities had set their units at a level that was too sensitive.

Metal Problems. Problems with detection occurred when the contraband was not metal; the number of these problems is expected to increase as the use of plastic increases. Another concern was the nearness of other metal that would cause false alarms. To allay this concern, walk-through detectors were placed from 2 to 15 feet (an average of 8.2 feet) away from metal door frames.

A unique consideration presented by walk-through detectors involved a l-foot free zone at the bottom of the archway that made it difficult to discover shanks carried by inmates in their shoes. One institution resolved this complication by placing ramps leading to and from the detectors that raised the feet of the person walking through to a level at which metal contraband in shoes could be detected.

Environmental Factors. In addition to problems caused by nearby metal, weather conditions were problematical (see Table 3-12). Nine out of ten institutions did not use walk-through detectors outdoors. About one in four facilities (23 percent) that did have detectors outdoors, had to relocate devices to avoid weather-related nuisance alarms.

Down-Time

Just under a third (31 percent) of the walk-through detectors were backed up by an uninterrupted power source. Of these, 9 out of 14 could operate indefinitely; the other 5 could function for an average of 32 hours. Only four facilities reported that in a typical 30-day period their detector could not be used because it was inoperative; for these, the average down-time was 11 days.

Maintenance and Repair

Thirteen facilities reported that their walk-through detectors broke down every 2.4 days, but for the group of 25 institutions that responded to this question, the average time between breakdowns was 162.7 days. Preventive maintenance was practiced by only 39 percent of the facilities reporting.

Providing maintenance and repair was most often the responsibility of staff (63 percent of the cases), though sometimes it was supplied by an outside contractor (33 percent). Where institution personnel performed the maintenance and repair work, a third (32 percent) thought a maintenance contract would be less expensive, while 40 percent thought the quality of repairs might improve with a maintenance contract.

Twenty-one percent of the institutions stocked spare parts for the key components of their walk-through detectors. The remaining 79 percent claimed that parts were readily available from the factory or dealer.

Training

Most institutions (77 percent) where staff were responsible for maintaining walk-through detection equipment did not have formal training classes. Because only four institutions provided information on these survey items, additional information concerning training cannot reported.

Testing

Staff or outside vendors (80 percent and 20 percent, respectively) tested walk-through detectors regularly in the sample facilities. Most often this testing was performed on a daily basis (in 87 percent of the institutions); however, in at least one instance, this testing occurred on every shift. As with hand-held detectors, staff believed that any problems with walk-through detectors would become apparent in the course of daily use.

X-RAY MACHINES

While 66 percent of the respondents had X-ray machines, most institutions had only one unit (36 out of 37). For the most part, these machines allowed complete visibility (81 percent), and the shapes and forms were distinct enough for identification (89 percent).

Eighty-six percent of the replies indicated that X-ray machines were essential to the security of the facility. These respondents all believed that without these devices contraband would be much more likely to enter the facility.

Problems

Eighty-five percent of the facilities equipped with X-ray machines installed them to inspect incoming packages. Only one administrator thought the penetration capability of the machines was not powerful enough. In 47 percent of the sample institutions, the X-ray machines were not large enough to handle the size of some objects that had to be examined. An additional concern was the lack of image clarity on some machines. In nine out of ten cases, the machine solved the problem for which it was installed.

All institutions had been assured that the level of X-ray dosage emitted by their machines was safe for staff operators.

Maintenance and Repair

An outside contractor was just as likely as institution personnel to maintain and repair X-ray machines (each used by 43 percent of the respondents), though manufacturers also played a role (32 percent) in this area. Where staff did the work, 40 percent of the administrators thought costs could be lowered by using an outside contractor, and 45 percent concluded the quality of repairs would be better.

Preventive maintenance for X-ray machines was performed by 39 percent of the responding institutions. The breakdown rate varied from once every 2 days to once every 6 years. Only 15 percent of the responding facilities stored spare parts for their X-ray machines, perhaps because 74 percent indicated they could get parts easily from the factory or dealer.

Testing

About three out of four institutions (74 percent) tested their X-ray machines regularly, most on the average of six times a week. Testing was usually done by staff (81 percent), though sometimes by an outside contractor (16 percent), and occasionally by a vendor (3 percent).

Training

Only 21 percent of facilities had established training classes for staff to learn X-ray maintenance and repair. Since only four institutions provided data, additional information concerning training cannot be reported.

DRUG-DETECTION CANINES

For the 18 facilities that had their own drug-detection canine teams, the average number of teams was three (one facility had ten). As shown in Table 3-13, German shepherds were the most popular breed (59 percent), followed by Labrador retrievers (28 percent), and bloodhounds (21 percent). Institutions without their own canine teams borrowed them from the central office, a neighboring institution, or a regional canine unit.

Table 3-13
Breeds of Drug-Detection Canines

	No. of Facilities	%*
German Shepherds	17	59
Labrador Retrievers	8	28
Bloodhounds	6	21
Other	6	21

* The total percentage exceeds 100 because a number of institutions reported using more than one breed of dog.

Uses

Canine teams were commonly used for building searches (90 percent), to detect concealed narcotics (86 percent), and to track evidence (48 percent). Some institutions (31 percent) used them as part of perimeter security to prevent escapes. Other uses for dogs were to accompany escorts on medical trips, to patrol visiting rooms, to track escapees, to assist in crowd control, to subdue riots, to detect explosives, to aid in grounds control, and to search cars. About two-thirds of the reporting facilities (64 percent) considered drug-detection canines an integral part of their total security package.

Qualifications and Training

Forty-eight percent of the sample institutions reported that applicants to staff the canine unit had to meet special qualifications; in 95 percent of the facilities the dogs also had to meet certain certification requirements. New canine handlers took a special training course in 57 percent of the facilities. In all cases the handlers were personally responsible for the care and feeding of their animals. Usually the animals lived with the handler (69 percent); the rest resided at the facility. Most of the institutions (78 percent) had policies regarding the use of canines.

Problems

Only one out of four facilities with canine units had any problems using them. Some just did not have enough dogs. Others reported transition problems when a handler was promoted. Veterinarian bills sometimes presented problems when cost was a consideration. Moreover, dogs were effective only a limited number of hours each day. Liability issues were also a concern; attack dogs could not be used in close quarters.

Conclusions and Issues

CONCLUSIONS

On the whole, the institutions surveyed were satisfied with the measures they had taken to reduce violence and escape attempts by detecting the introduction and the movement of contraband within their perimeters. Staff were released for other assignments when detection equipment and dogs were used to search people and parcels entering into the facility. The deterrent psychological effect of internal detection equipment was specifically cited as a virtue in 15 percent of the replies.

During an onsite visit, facility staff reported an interesting example of the deterrent value of detection equipment. This facility required inmates to walk through detectors when they passed from one area in the institution to another. Because anyone stopped for setting off the detector would hold up the line, peer pressure changed the behavior of inmates: Not only were they unlikely to carry anything that would activate the alarm, they removed belts, shoes, and anything else that might set it off.

Metal detector units were the most prevalent type of internal detection system in use, despite one obvious shortcoming: They did not detect nonferrous objects such as drugs. Dogs, searches by facility staff, and informants were the methods used most successfully to detect illegal drugs, the single most likely type of contraband to be confiscated.

Hand-held detectors, the most popular technology, were rated the most effective for the following reasons:

- While the cost of X-ray machines and walk-through detectors could run into thousands of dollars, the cost of hand-held detectors was a maximum of several hundred (one model was available for $15).
- Because they are portable, hand-held detectors could be used to search a wide variety of objects and could be taken to the people or the articles to be searched rather than having the people or objects come to them.
- They locate contraband more specifically than walk-through detectors.

Though hand-held detectors were considered the most useful, they were not used exclusively. The other forms of detection equipment, as well as the canine units, had advantages in certain situations (e.g., when used in conjunction with random searches).

Generally, facilities relied more on staff than on either equipment or dogs as the front line for internal security.

ISSUES

Based on the information provided by the survey data, a number of issues emerged that administrators need to consider when internal detection systems are being designed or upgraded:

1. Prepare a list, with input from staff, of the requirements that a new system should meet now and during the next 5 to 10 years. Your list should answer at least the following questions:

   a. Will the detection system be used more for its deterrent value than to actually detect contraband?
   b. Will the system detect the type of contraband that is most prevalent in your facility?
   c. Has the amount of metal in the building been taken into consideration?
   d. Has staff had input in regard to where the new system will be located?
   e. If the system is to be used outside, has consideration been given to its susceptibility to the elements?
   f. Will the detection system be used in conjunction with random searches?

2. Check decisions with colleagues in other institutions/systems to benefit from their experiences; learn the weaknesses of each system.

3. Purchase equipment for which parts will be readily available, and remain available, once the system is installed, and for which there are local contractors who can provide 24-hour service.

4. Check the plans for the detection system's installation prior to activation.

5. Determine whether the facility has the appropriate electrical wiring for the system (or systems) being considered.

6. Integrate new systems with existing ones. Test the system components in situations that simulate actual operations.

7. Have a trained staff member monitor the installation to ensure that the installers are properly trained and working appropriately.

8. Determine whether or not the system has a good warranty, one that is explicit as to what is covered.

9. Plan to conduct defeat-testing of the system, post-installation, in situations that simulate actual operations.

10. Ensure that the installer, vendor, and/or manufacturer is under a performance bond. Determine how the bond will be enforced in the event there are problems with the system.

11. Have the vendor provide detailed drawings of the system, after it is in place, to simplify maintenance and repair.

12. Obtain schedules for maintenance and repair from the manufacturer, vendor, and/or installer, and a schedule for (and information on) appropriate testing methods.

13. Determine whether or not maintenance and repair of the system will be accomplished by facility staff or by a maintenance contract.

14. Plan for staff to be trained in how to operate, maintain, and repair the system. Try to arrange the training as part of the sales contract.

15. Plan how follow-up training will be provided for both present personnel and new hires.

16. Consider whether or not this system is necessary to answer the needs of the institution or whether it is a case of upgrading for upgrading’s sake.

Chapter 3

Questionnaire Data-Internal Detection Systems

Hand-Held Metal Detectors	55	X-Ray Machines	37
Walk-Through Metal Detectors	52	Drug-Detection Canines	29
Other (specify)	18		

1. What three types of contraband are detected most frequently? List them in order from the most frequently detected to the least frequently detected. (If drugs, please list type if known. If weapon, please list type, e.g. metal shanks, etc.) (covered in text)

2. Please rank walk-through detectors, hand-held detectors and X-ray machines in order of their effectiveness in detecting contraband. List them in order from most effective to least effective. (covered in text)

3. Are the internal detection systems at this facility part of an overall, integrated security system?
Yes 32 No 22 Don't Know 1 No Response 1

4. How many shanks (prison made knives) were confiscated, with the aid of detectors, during the past year?
# of Responses - 16 Average # of Shanks - 13.31 High 58 Low 1

5. How many shanks were confiscated, without the aid of detectors, during the past year?
# of Responses - 46 Average # of Shanks - 33.83 High 180 Low 1

Hand-Held Detectors
(55 Responses)

1. Do your hand-held detectors feature an automatic reset system?
Yes 36 No 16 Don't Know 3

2. The signal is [Check (x) ONE]

Audible	30
Visible	0
Both	24
Don't Know	0
No Response	1

3. Can scanning be accomplished silently?
Yes 22 No 31 Don't Know 2 No Response 0

4. Do the hand-held detectors alarm for nonferrous objects?
Yes 10 No 38 Don't Know 6 No Response 1

5. Are the hand-held detectors durable?
Yes 46 No 7 Don't Know 1 No Response 1

6. Hand-held detectors are used to search [Check (x) ALL that apply]

Mattresses	38
Linens	28
Packages	27
People	54
Other (specify)	6

7. Hand-held detectors are used to search [Check (x) ALL that apply]

Inmates	49
Visitors	47
Staff	28
Vendors	35
Other (specify)	3

8. Are the hand-held detectors are reliable?
Yes 49 No 4 Don't Know 2

9. The hand-held detectors are essential to the security of the facility?
Yes 41 No 12 Don't Know 2

10. If yes, what would be the effect on the security of the facility if they were removed? (covered in text)

11. How many hand-held detectors does the facility have?
# of Responses - 51 Average # of Hand-Held Detectors - 9.43 High 40 Low I
Don't Know 3 No Response 1

12. Does this number include spare units that can be used while others are being repaired or recharged?
Yes 37 No 15 Don't Know 2 No Response 1

13. Were the hand-held detectors acquired for a particular reason or to solve a specific problem?
Yes 29 No 21 Don't Know 5 No Response 0

14. If the hand-held detectors were purchased for a specific reason, what was the reason? (covered in text)

15. Have the hand-held detectors met the expectations in terms of solving the problem?
Yes 37 No 5 Don't Know 8 No Response 5

16. If they did not solve the problem, why? (covered in text)

Walk-Through Metal Detectors
(52 Responses)

1. How long have you had the walk-through detection system?
# of Responses - 1 Average # of Months - 6 High 6 Low 6
# of Responses - 49 Average # of Years - 8.2 High 19 Low 2

2. How many walk-through detectors does the facility have?
# of Responses - 51 Average # Detectors - 2.49 High 13 Low 1

3. Where is/are the walk-through detector(s) located? [Check (x) ALL that apply]

All entrances to facility	29
Entrance to visiting room	19
Between cell houses	19
other (specify)	36

4. Is the walk-through detector an integral part of the total security package?
Yes 44 No 7 Don't Know 0

5. If yes, what would be the effect on the security of the facility if the system was removed? (covered in text)

6. The walk-through detector is used to search [Check (x) ALL, that apply]

Inmates	39
Visitors	51
Staff	32
Vendors	44
other (specify)	4

	Yes	No	Don't Know	No Resuonse
7. Will the detector expose objects regardless of shape, position or orientation?	40	6	6	0
8. Will the detector expose objects even if a person is moving through it rapidly?	42	6	4	0
9. Can the detector be reset automatically as well as manually after an alarm?	47	**3**	2	0
10. Was the detector tamper-resistant as delivered?	27	**8**	17	0
11. Has anything been done to make the walk-through detector more tamper-resistant than when it was delivered?	14	33	5	0

12. If yes, what was done to make the detector more tamper-resistant? (covered in text)

13. Is the detector backed up by an uninterrupted power system?
Yes 15 No 33 Don't Know 3 NoResponse 1

14. If yea, how long can the uninterrupted power system operate the walk-through detector system?
# of Responses - 5 Average - 32.2 Hours High 96 Low 2

15. During a typical 30-day period, estimate the number of days the walk-through detector is NOT being used because it is inoperative.
# of Responses - 4 Average - 10.75 Days High 30 Low 2

	Yes	No	Don't Know	No Response
16. Can the detector be upgraded as advances in technology are made?	9	18	25	0
17. Is the detector used out of doors as well as inside?	5	47	0	0
18. Has it been necessary to relocate the units to prevent nuisance alarms caused by environmental factors?	12	40	0	0

19. How close are walk-through detectors to metal door frames or entrances?

# of Responses - 52   Average - 8.15 Feet   High 15   Low 2

20. What three environmental factors cause nuisance alarms most frequently? List them in order with #l representing the most disruptive factor and #3 representing the least disruptive factor. (covered in text)

21. Does the facility experience false alarms with the walk-through detectors? (i.e., alarms caused by system malfunctions)

Yes 18   No 33   No Response 1

22. False alarms are typically due to [Check (x) ALL that apply]

Installation Problems	7
Equipment Problems	14
Other (specify)	16

23. Were the walk-through detectors installed in this facility for a particular reason or to solve a specific problem?

Yes 34   No 14   Don't Know 4

24. If the walk-through detectors were installed for a specific reason, what was the reason? (covered in text)

25. Have the walk-through detectors met expectations in terms of solving the problem?

Yes 33   No 3   Don't Know 7   NoResponse 9

26. If they did not solve the problem, why? (covered in text)

X-Ray Machines
(37 Responses)

1. How many X-ray machines does the facility have?

# of Responses - 37   Average # of Machines - 1.3   High 3   Low 1

	Yes	No	Don't Know	No Response
2. Is the penetration capability of the X-ray machine(s) powerful enough?	35	2	0	0
3. Do/does the X-ray machine(s) allow complete visibility?	30	7	0	0
4. Are the shapes and forms seen distinct enough for identification?	33	4	0	0
5. Is the X-ray dosage safe for operators?	36	0	1	0
6. Is/are the X-ray machines large enough to handle any size of object that may need to be examined?	19	17	1	0
7. Is/are the X-ray machines essential to the security of the facility?	32	5	0	0

8. If yes, what would be the effect on the security of the facility if the machine(s) was/were removed? (covered in text)

9. Were the X-ray machines installed for a particular reason or to solve a specific problem?
Yes 29 No 5 Don't Know 3

10. If the X-ray machines were installed for a specific reason, what was that reason? (covered in text)

11. Have the X-ray machines met expectations in terms of solving the problem?
Yes 27 No 3 Don't Know 3 No Response 1

12. If they have not solved to problem, why? (covered in text)

Drug-Detection Canines
(29 Responses)

1. If yes, how many canine teams does the facility have?
# of Responses - 18 Average # of Canine Teams - 2.94 High 10 Low 1

2. What breed(s) of canines are used by the facility? (covered in text)

3. What are the canine teams used for? [Check (x) ALL that apply]

Building searches	26
Prevent escapes	9
Track evidence	14
Detect presence of concealed narcotics	25
Other (specify)	7

	Yes	No	Don't Know	No Response
4. Does the facility have an established policy of qualifications of applicants for the canine unit?	12	13	3	1
5. Are there established certification requirements for all dogs in the canine unit?	20	1	3	5
6. Does the facility have a prescribed canine training course for new canine handlers?	12	9	3	5
7. Does the facility have established policies regarding the use of canines?	18	5	3	3
8. Are the canine handlers personally responsible for the care and feeding of their animal?	22	0	1	6

9. If no, who is responsible for the animals? (covered in text)

10. The animals live [Check (x) ONE]

With handler	16
At the facility	8
Other (specify)	2
No Response	3

11. Is the use of drug-detection canines an integral part of the total security package of the facility?
Yes 18 No 10 Don't Know 0 No Response 1

12. Are there problems associated with the use of canines in the facility?
Yes 6 No 18 Don't Know 2 No Response 3

13. If yes, please list the three major problems. (covered in text)

General Information

1. The detectors are [Check (x) ONE]

	Walk-Through Detectors	Hand-Held Detectors	X-Ray Machines
Leased	0	0	0
Purchased	51	53	36
Don't Know	1	1	0
No Response	0	1	1

	Walk-Through Detectors	Hand-Held Detectors	X-Ray Machines
2. Who is responsible for the maintenance and repair of the internal detection **systems** [Check (x) ONE]			
Staff	33	30	16
Manufacturer	10	14	12
Outside Contractor	17	14	16
Leasing Company	0	0	1
0ther (specify)	0	0	0
3. If staff, does the facility have an established training class for staff to learn maintenance and repair?			
Yes	8	7	5
No	27	29	19
No Response	17	19	13
4. How many hours of training in maintenance and repair are required for staff?	Responses 4 Average 16 High 40 Low 6	Responses 4 Average 13.50 High 40 Low 2	Responses 3 Average 16.67 High 40 Low 2
5. What percentage of staff are trained to maintain and repair the internal detection systems?	Responses 21 Average 7.38 High 50 Low .01	Responses 18 Average 6.67 High 50 Low .01	Responses 12 Average 2 High 10 Low 1
6. Does the facility have preventive maintenance programs for detectors?			
Yes	19	14	12
No	30	34	19
No Response	3	7	6

7. What is the average amount of time, per year, between breakdowns?

Walk-Through Detectors

Days
# of Responses - 13
Average # of Days - 2.38
High 7 Low 1

Weeks
# of Responses - 1
Average # of Weeks - 6
High 6 Low 6

Months
# of Responses - 8
Average # of Months - 6.13
High 9 Low 2

Years
# of Responses - 3
Average # of Years - 2
High 4 Low 1

Hand-Held Detectors

Days
# of Responses - 5
Average # of Days - 2.80
High 7 Low 1

Weeks
# of Responses - 4
Average # of Weeks - 3
High 6 Low 1

Months
# of Responses - 8
Average # of Months - 5.38
High 10 Low 1

Years
# of Responses - 2
Average # of Years - 1
High 1 Low 1

X-Ray Machines

Days
# of Responses - 5
Average # of Days - 3.80
High 7 Low 2

Weeks
# of Responses - l
Average # of Weeks - 1
High 1 Low 1

Months
# of Responses - 3
Average # of Months - 4.67
High 8 Low 3

Years
# of Responses - 4
Average # of Years - 3
High 6 Low 1

	Walk-Through Detectors	Hand-Held Detectors	X-Ray Machines
8. The training is provided by [Check (x) ALL that apply]			
Vendor	10	6	9
Facility	23	26	16
Manufacturer	8	7	5
Other (specify)	3	2	1
No Response	8	14	6
9. If staff now performs maintenance/ repairs, do you believe a maintenance contract would be an improvement?			
(a) For Cost			
Yes	10	9	6
No	21	21	9
Don't Know	3	5	4
No Response	18	20	18
(b) Quality of Repairs			
Yes	10	9	5
No	15	16	6
Don't Know	8	9	7
No Response	19	21	19
10. Does the facility stock spare parts for the key components of the internal detection systems?			
Yes	10	7	5
No	37	41	28
No Response	5	7	4

	Walk-Through Detectors	Hand-Held Detectors	X-Ray Machines
11. Are spare parts readily available from the factory or dealer?			
Yes	33	33	23
No	9	10	8
No Response	10	12	6
12. Does the facility have regularly scheduled testing of the systems?			
Yes	33	31	23
No	12	14	8
Don't Know	2	3	0
No Response	5	7	6

13. If yes, how often is/are the systems tested? [Indicate number of times on line and check (x) the time.]

Walk-Through Detectors

Weeks
# of Responses - 27
Average # of Weeks - 6.63
High 21 Low 1

Months
# of Responses - 3
Average # of Months - 2.23
High 4 Low 1

Years
# of Responses - 1
Average # of Years - 2
High 2 Low 2

Hand-Held Detectors

Weeks
# of Responses - 25
Average # of Weeks - 5.88
High 21 Low 1

Months
# of Responses - 1
Average # of Months - 2
High 2 Low 2

Years
# of Responses - 2
Average # of Years - 46
High 90 Low 2

X-Ray Machines

Weeks
# of Responses - 20
Average # of Weeks - 5.65
High 21 Low 1

Months
# of Responses - 1
Average # of Months - 2
High 2 Low 2

Years
# of Responses - 1
Average # of Years - 2
High 2 Low 2

14. Who tests the equipment?

	Walk-Through Detectors	Hand-Held Detectors	X-Ray Machines
Staff	37	34	25
Vendor	0	0	1
Outside contractor	6	5	5
Other (specify)	0	0	0
No Response	9	16	6

Chapter 4

Monitoring and Surveillance Systems in Correctional Facilities

Abstract

Correctional Technology: A User’s ***Guide*** is the product of a nationwide assessment of the experience correctional administrators have had with various types of technological systems. The purpose of this guide is to provide correctional administrators with a user-friendly source of information to aid planning and decisionmaking.

For this chapter on monitoring and surveillance systems, survey questionnaires were prepared, reviewed by corrections monitoring and surveillance experts, pilot-tested onsite, and revised in light of that input. The final version was sent to 58 correctional institutions, selected to represent all areas of the country and all levels of security. Presurvey letters and follow-up telephone calls resulted in an 86 percent response rate.

Closed-circuit television, the most common monitoring and surveillance equipment, was used by 90 percent of the respondents. However, the finding that one staff member was asked to monitor an average of six screens at a time, each of which switched between an average of six cameras, suggests that this technology was not being used appropriately.

Corrections officials regard monitoring and surveillance equipment as essential to their work. The survey data suggest the need for better coordination between the designers, installers, and operators of these systems.

Table of Contents

LIST OF TABLES

Executive Summary

Fifty facilities, representing an 86 percent response rate, returned the Monitoring and Surveillance Systems questionnaire. For the 48 U.S. institutions, the distribution across the country was fairly even. In terms of security levels among the sample institutions, the medium and mixed facilities had the highest representation (28 percent each). In addition, the sample facilities were relatively new (62 percent opened since 1980) and of intermediate size (38 percent with 500 to 999 inmates).

In general, although correctional administrators were satisfied with their equipment, the data suggest that there was little interaction among the designers, installers, and equipment operators during the planning and installation of most of the systems.

CLOSED-CIRCUIT TELEVISION

The most common monitoring and surveillance system among the sample institutions was closed-circuit television (CCTV), used by 90 percent of the respondents. Eighty-two percent of the replies indicated CCTV was essential to the security of the facility. Per facility, the average number of monitoring screens was 14, each of which monitored, on average, six cameras. The average number of screens watched by one staff member was six. All of these individuals also had additional duties (e.g., monitoring control panels, issuing keys and equipment, answering telephones, and escorting high-security inmates). This set of circumstances raises an important question: Were CCTV systems being used effectively?

Although 78 percent of the facilities reported a desire for additional cameras, the data suggest that the need might be less for cameras than for better planning-preferably, with decisions based on a time-motion study. Other conditions affecting the utility of CCTV pertained to bugs in the systems after they were installed and the negative effect of some environmental conditions, such as bright light, fog, and darkness. Inmate tampering problems were minimal.

MOTION DETECTORS

Eighty-three percent of all respondents considered motion detectors essential to institution security; they were used by 58 percent of the sample institutions. However, motion detection technology was susceptible to false alarms. The average false alarm rate for the sample institutions was one every 8.4 days. For the sample facilities, the average debugging time was 16.4 months (range from 5 days to 8 years). In more than one out of four cases (27 percent) the system was never successfully debugged.

In addition to installation difficulties, poor design and the fact that motion detectors did not interface with other monitoring and surveillance equipment also caused problems. Animals presented a big problem for motion detection technology (mentioned by 54 percent of the respondents), as did hail and blown debris.

ACCESS-CONTROL DEVICES

Access-control technology is relatively new in corrections. The two most prevalent approaches used by the 17 facilities (34 percent) that had this technology were push-button, key-pad code systems (41 percent), and punched-card access systems (30 percent). Other access-control systems used included electrical lock override systems, audio identification systems, and door and gate control panels.

Eighty-six percent of these 17 facilities indicated that access-control technologies were essential to their facilities' security. Had they not been installed, more staff would have been needed, security locks would have had to be installed, there would have been no automatic record of security rounds, and aid to injured or endangered officers in master control would have been delayed.

In 85 percent of the responding facilities the access-control system was tamper-resistant when installed. Seventy-one percent of the responding institutions had debugging to do after their system was installed.

AUDIO-MONITORING SYSTEMS

Although 30 (60 percent) of the respondents had audio-monitoring systems, only 6 answered all the items in that section of the questionnaire. Consequently, the data for audio-monitors had more anecdotal than statistical validity and cannot be reported on here (see instead the Questionnaire Data at the end of this section).

Introduction

On the theory that the best way to control inappropriate behavior is to prevent it, correctional administrators have turned to the use of monitoring and surveillance technology. The Monitoring and Surveillance Systems questionnaire was sent to 58 correctional institutions; 50 responded, giving an 86 percent response rate.

The primary intent of this technology is to prevent access to, and/or alert staff when intruders (inmates or nonauthorized individuals) are in, off-limits areas. Use of monitoring and surveillance systems reduces the likelihood of escapes and diminishes threats to the orderly running of the facility. Thus, these systems help protect inmates from one another and aid in the prevention of disturbances within institutions.

According to the survey data, the most commonly used monitoring and surveillance technology was closed-circuit television (CCTV) (90 percent), followed by audio-monitoring (60 percent), motion detectors (58 percent), and access-control systems (34 percent); access-control systems include push-button and punched-card methodologies.

The objective of this chapter is to provide corrections administrators with information relevant to decisionmaking about monitoring and surveillance systems technology. It includes the following:

- A description, in nontechnical terms, of the types of technology in use;
- An indication of support systems and staff needed to install, operate, and service the various systems;
- Factors to be considered during the selection and planning for the use of technology; and
- Conditions under which particular technologies may be appropriate, reliable, effective, or efficient.

This chapter contains the following:

- An overview of monitoring and surveillance systems technologies,
- A description of the characteristics of the institutions sampled in the survey,
- An analysis of the survey findings,
- Conclusions drawn from survey results, and
- Issues to consider when evaluating a monitoring and surveillance system.

Monitoring and Surveillance Systems: An Overview

Monitoring and surveillance systems provide institution personnel with technology that enables them to better control access to off-limits areas within the facility. The major systems being used are closed-circuit TV (CCTV), motion detectors, access-control devices, and audio-monitors.

CCTV, found in nine out of ten of the responding facilities, is an arrangement in which television cameras, placed in potentially vulnerable areas within an institution, can be monitored by staff usually located in a control center. For responding institutions, typical camera locations were at entrances and sally-ports, in visiting areas, and along the facility's perimeter.

Motion detectors, found in 58 percent of the responding facilities, use infrared light waves, radio frequency transmission, ultrasound, or microwaves to detect changes that occur in a previously empty space when a human body enters it. They detect a change in volumetric pressure or temperature changes as a consequence of radiant body heat. (See also the discussion of motion sensors in Chapter 1, "Perimeter Security Systems.")

When radio frequency waves are used, the false alarm rate can be high, because the waves may penetrate walls and respond to motion outside the designated area unless the walls are shielded. Some of these devices can be adjusted by skilled technicians to tune out motion outside the protected area.

Ultrasonic detectors operate in a fashion similar to radio frequency systems; however, they do not penetrate walls. They are not affected by audible noise itself, but such noise can sometimes disturb wave patterns and create false alarms.

Access-control systems allow certain designated persons to enter otherwise secured areas. Among the 17 facilities who reported using access-control systems, two types were prevalent: push-button code (16 percent) and card-access-control (10 percent).

Push-button code systems have keypads installed at the entrance to each controlled-access area. Those authorized to enter are given the combination to be punched into the keypad. There is no keyhole to allow locks to be picked, and locks are easily recoded if prior combinations have been compromised or when there are staff changes.

Card-access-control systems use card readers instead of keypads. Authorized individuals are given programmed cards that allow entrance into a given area. Magnetic key-card systems use a plastic card containing thousands of magnetic bits or particles that are arranged to match the pattern set up in the card reader. When a match is made, the locking system is activated. This system can easily be converted into a total, facility-wide system with the following advantages:

- Key cards can be coded by the facility for use by staff and/or inmates.
- The system can require a coded series of numbers to match the presented card before granting entry.
- The system can generate a printout showing who entered an area, the time and date of

entry and exit, and the identity of the areas in which the card was used.

- The system can reject, but record, cards presented for entry into unauthorized areas. Additionally, an audio alarm installed at the control center can be triggered.
- The system can be designed so that key cards will be honored only between designated time periods.
- If necessary, the system can be designed to deny access to a particular card.
- Cards issued to inmates can be tied into data processing for commissary or library use.
- Cards can be coded to prevent them from being used by more than one person (e.g., a card used to enter an area would have to be used to exit the area before it could be used to enter again).

Audio-monitors, reported in six out of ten responding institutions, were sometimes installed as part of a CCTV or intercom system. This technology is similar to CCTV, but rather than conveying an image, it picks up and transmits sound through a closed-circuit audio system to one or more locations staffed by institution personnel.

Existing public address systems, with the speaker turned into a microphone, can listen to sounds in the protected area and then trigger an alarm relay when an intrusion takes place. The output of individual audio amplifiers can be adjusted to prevent activation of the alarm by normal noises when the area is unoccupied.

The false alarm rate can be reduced by using two microphones, one within the protected area and one outside it. Within the circuit, the noise signals are equalized in relation to a typical noise level for each of the microphones. If an intruder enters the protected area, one microphone will pick up the additional noise and the other microphone will not. The unequal noise levels will set off an alarm.

Another method for reducing audio-monitor false alarms employs complex audio filters. Any recognizable sound has a distinct acoustic spectrum. The audio signal developed by a microphone placed in a protected area is processed through a series of audio-frequency filters tuned to let through signals at certain frequencies and reject others not in the area of interest. Certain band-pass filters can detect a difference between human intrusion noises and other noises of no interest for security purposes.

Sample Characteristics

Fifty of the 58 facilities (86 percent) that where sent the monitoring and surveillance systems survey provided data concerning the prevalence and concerns regarding these systems.

LOCATION AND SECURITY LEVELS

Table 4-l shows the distribution of the 48 U.S. institutions that responded. The distribution across the country was fairly even, with most located in the Midwest (33 percent), followed by the South (27 percent), the West (23 percent), and the Northeast (17 percent).

Table 4-2 shows the security level of the sample institutions; medium and mixed (inmate population less than two-thirds in any category) institutions had the highest representation (28 percent each). Twenty-six percent were minimum security, and 18 percent were maximum security (long- term, difficult inmates). In general, the security levels were fairly equally represented.

Table 4-1
Location of Sample Facilities

Location	n	%
Northeast	8	17
South	13	27
Midwest	16	33
West	11	23
Total*	48	100

* Excludes two additional Canadian facilities that responded to this survey.

Table 4-2
Security Level of Sample Facilities

Security Level	n	%
Minimum	13	26
Medium	14	28
Maximum	9	18
Mixed*	14	28
Total	50	loo

* Inmate population was less than two-thirds in any category.

AGE OF SAMPLE FACILITIES

As shown in Table 4-3, most of the responding facilities were quite new (62 percent had opened since 1980), although six were built before 1900.

POPULATION SIZE OF SAMPLE FACILITIES

Sample institution size is shown in Table 4-4 as the average daily population (ADP). The majority of the facilities (38 percent) had an ADP of between 500 and 999.

In summary, the average respondent was from a fairly new, midsized, midwestem institution, holding medium or mixed security inmates.

Table 4-3
Date Facilities Opened

	n	%
Before 1900	3	6
1900-1939	6	12
1940-1979	10	20
1980-Present	31	62
Total	50	100

Table 4-4
Average Daily Population

Population	n	%
Under 500	17	34
500-999	19	38
1000+	14	28
Total	50	100

Survey Findings

Corrections administrators reported a variety of technologies were used to detect intrusions into unauthorized areas. Table 4-5 shows usage frequency; for example, 90 percent of the sample facilities used closed-circuit television (CCTV). Audio-monitors and motion detectors were both used by more than half of the respondents (60 percent and 58 percent, respectively). Since respondents were encouraged to select ***all*** that applied, the percentages reported add up to more than 100 percent.

CLOSED-CIRCUIT TELEVISION

While CCTV was not a new technology for correctional institutions (the average age of in-place systems was 6 years), 82 percent of the replies indicated it was essential to the security of the facility. If the CCTV system was removed, 43 percent of the respondents claimed additional staff would be needed, 37 percent that security would be compromised, and 31 percent that special housing units could not be monitored.

About half (49 percent) of the CCTV systems were used to record rule violations. Only 43 percent of these systems had built-in recording capability, and of these, 15 percent recorded continuously; for the others, recording had to be started manually in 80 percent of the cases, while the remaining 5 percent had automatic start-up.

Table 4-5
Internal Detection Systems - Usage

	No. of Facilities	%*
CCTV	45	90
Audio-Monitors	30	60
Motion Detectors	29	58
Push-Button Codes	8	16
Punched-Card Access	5	10

* The total percentage exceeds 100 because a number of respondents reported using more than one internal detection system.

System Effectiveness

In nine out of ten instances, the administrator had a particular reason for installing CCTV. For more than half (58 percent), it was a desire to get better inmate observation without increasing staff; others (42 percent) wanted to improve security. Usually (in 91 percent of the cases) the CCTV system solved the problem for which it was installed. Where it did not, the reasons given were poor quality equipment, the need for camera upgrading, or the need for more cameras.

Cameras and Monitoring Screens

The number of cameras and monitoring screens varied widely. For cameras, the number per facility ranged from 1 to 125, the average being 21. The average number of monitoring screens was 14 (ranging from 1 to 150). Most (89 percent) were monochrome. These camera and monitor figures show that in 84 percent of the facilities one screen monitored more than one camera. Administrators at 78 percent of the reporting facilities would like more cameras.

The average number of cameras monitored by one screen was 5.5, but the high was 50. This finding raises a focal question: Does the image from one camera stay on screen long enough for the person monitoring to react to it?

A second pivotal issue concerned the number of screens monitored by one staff member; the average number was 5.8, with a high of 18. Since staff members had additional duties, how attentively could a staff member monitor six or more flickering TV images?

Almost invariably (in 98 percent of the institutions), staff who monitored CCTV screens had other duties. They either operated doors and gates (30 percent), monitored radios (17 percent), had key (15 percent) or property control (5 percent) responsibilities, staffed the reception desk (12 percent), handled booking (5 percent) or intake (4 percent), did counts (4 percent), maintained the log book (4 percent), or supervised the visiting room (2 percent) or other staff (2 percent).

In more than six out of ten sample institutions (64 percent), CCTV cameras were monitored in more than one location. Screens were either in a control room (50 percent-includes the 36 percent single sites), segregation unit (20 percent), housing unit (8 percent), visiting room (8 percent), admission/orientation unit (5 percent), main gate sally-port (5 percent), or in one or more towers (3 percent). On average, three staff members monitored the surveillance cameras on every shift (3.1 on morning, 2.9 on afternoon, and 2.5 on midnight).

Installation

More than half (58 percent) of the facilities reported bugs in their CCTV systems after installation. The time needed to correct these problems ranged from 3 days to 4 years (average was 3.8 months).

CCTV systems were usually (78 percent) installed by outside contractors, though sometimes by the manufacturer or the facility’s staff (11 percent each). A performance bond was required of the contractor, manufacturer, and/or vendor by 86 percent of the respondents. Administrators reported that using several contractors could significantly interfere with security equipment compatibility.

Maintenance

Just over a third (37 percent) of the responding institutions had scheduled maintenance and testing programs for their CCTV systems. These included weekly visual inspections as well as annual cleaning. Eighty-six percent of the respondents who followed a regular maintenance schedule reported they did not have many problems that required repairs. Of the facilities that used a random approach, 71 percent made repairs as needed; of these, 15 percent tested daily, and 14 percent did a daily visual check.

Maintenance work was more likely (56 percent) to be done by staff, who were responsible for testing (49 percent), maintaining (39 percent), cleaning (9 percent), and visually checking (4 percent) equipment.

Just over half (53 percent) of the institutions stored spare parts for their CCTV systems;

96 percent indicated they could easily get parts from the manufacturer.

Problems

Lighting negatively affected CCTV screens according to 65 percent of the sample facilities. In these instances, most respondents (73 percent) stated that screen images were not easily visible; others reported problems with light reflection, resolution, or a lack of adequate lighting in the area under surveillance.

Inmates tampering with CCTV equipment was mentioned by only one (2 percent) of the respondents.

The most common repairs needed by CCTV systems are shown in Table 4-6.

Environmental conditions had a definite effect on some CCTV systems because 79 percent of them were used outdoors. Table 4-7 shows the vulnerability of these systems to environmental conditions. Three situations most detrimental to effective use of CCTV were bright light, fog, and darkness.

Table 4-6
Most Common CCTV Repairs

	No. of Facilities	%*
Replace		
Cameras	12	27
Burned-Out Tubes	2	5
Lens	2	5
Monitors	2	5
Static Boards	2	5
Adjust		
Camera Angle	7	16
Picture	6	44
Clean	6	14
Cable Connections	3	7
Defrosters	2	5

* The total percentage exceeds 100 because a number of respondents reported more than one kind of common CCTV repair.

MOTION DETECTORS

Types

Facilities that used motion detectors were partial to microwave sensors (72 percent), though a third (34 percent) used electric field sensors (see Table 4-8).

Placement

Motion detectors were most often used as part of the institution's buffer zone; for example, 41 percent placed them inside the perimeter fence (see Table 4-9). Other sites used for motion detectors were between fences and in sally-ports, both reported by 22 percent of the respondents. Recommendations for other areas that should be so equipped included around the power house, in the commissary, at external exit doors, around emergency generators, in loading and delivery areas, in recreation areas, and in the visiting area.

Table 4-7
CCTV - Vulnerability to Environment
(Conditions Ranked Most to Least)

Condition	Rank
Bright Light	1
Fog	2
Darkness	3
Snow/Ice	4
Wind	5
Temperature	6

Table 4-9
Motion Detectore - Usage

	No. of Facilities	%*
Microwave	23	72
Electric Field	11	34
Infrared	3	9
Thermal	1	3

* The total percentage exceeds 100 because a number of respondents reported using more than one type of motion detector.

Table 4-9
Placement of Motion Detectore

	No. of Facilities	%*
Buffer Zone		
Inside Perimeter Fence	13	41
Between Fences	7	22
Inside Perimeter Wall	2	6
Sally-Port	7	22
Rooftops	5	16
On Fence	4	12
Hallways	3	9
Building Attics	2	6
Warehouse	2	6
Other	3	9

* The total percentage exceeds 100 because a number of respondents reported more than one location for the placement of their motion detectors.

Security

Only four out of ten respondents who used motion detectors used them in conjunction with CCTV. Half of those that did ***not,*** thought such an integrated approach was a good idea. Eighty-three percent of all respondents considered motion detectors essential to the security of the facility. Eighty percent of the replies expressed concerns that without this technology security would be compromised, another 36 percent believed that they would need additional staff if they did not have motion detectors in place.

The alarms sent by motion detectors were usually (78 percent) a combination of audio and light, though 13 percent of the institutions had audio only. Some (19 percent) viewed the alarm on a computer screen display or printout. The alarm was most likely (59 percent of the time) to be received by staff in a control center; 34 percent of motion detector alarms were monitored not only by central control but also by patrols. Respondents seemed to believe that a perimeter system should have at least two alarms.

Installation

Motion detection systems were usually (73 percent) installed by an outside contractor, though sometimes the installer was the manufacturer (17 percent), or the facility's staff (10 percent). Ninety-four percent of the 28 respondents who answered the survey question about performance bonds said they required one of the installer. Only two answered whether or not the bonded installer was required to fix any post-installation problems that might develop; both indicated they "didn't know."

Training

Only two respondents answered the training questions, too small a sample for analyzing this data (see Questionnaire Data in Appendix section of this chapter).

Maintenance, Testing, and Repairs

The data showed a greater concern for testing and maintaining motion detectors than was the case for CCTV systems, although one respondent stated that both systems ***“are very simple and nearly maintenance free.”*** Sixty-nine percent of the respondents reported having scheduled testing and maintenance for the motion detector systems, compared with 37 percent who followed such a regimen for CCTV technology. For 66 percent of the facilities, staff did the testing; in about half (53 percent) they provided the maintenance.

Daily testing was routine in 50 percent of the facilities; at the extremes, one institution tested every 4 hours while another tested annually. However, performing maintenance and testing on a scheduled basis was not a panacea; 41 percent of institutions with schedules still reported problems.

Repairs most commonly required for motion detection technology were of damaged circuit boards (38 percent of the respondents). Other repairs frequently mentioned included those necessitated by poor equipment or installation (in 25 percent of the replies), sensitivity adjustments (19 percent), wiring (13 percent), and interfacing systems with each other (5 percent). Over 80 percent of the respondents thought an outside contractor would neither reduce costs nor improve the quality of repairs (82 percent and 89 percent, respectively).

Problems

False Alarms. Motion detection technology was susceptible to false alarms. Six replies reported daily false alarms (ranging from 50 times a day to 5 times per year). The average false alarm rate was one every 8.4 days. All respondents attributed their false alarm problems to equipment failures. Some (29 percent) referred specifically to installation difficulties, while others (36 percent) cited sensitivity maladjustments or interfacing problems.

Nuisance Alarms. Nuisance alarms, stemming from natural causes, were reported by nine out of ten institutions. The average nuisance alarm rate for the sample institutions was about 4.4 per week.

Animals presented the biggest problem; 54 percent reported that their motion detection system was “affected,” and another 27 percent said it was “somewhat affected” by animals. Hail and blowing debris were also high on the list (see Table 4-10).

Table 4-10
Motion Detectors - Vulnerability to Environment
(Conditions Ranked Most to Least)

Condition	Rank
Animals	1
Hail	2
Blowing Debris	3
Snow/Ice	4
Wind	5
Lightning	6
Rain	7
Temperature	8

Failure To Meet Expectations. Almost all (98 percent) of the respondents installed motion detection systems to address a particular situation, most often (88 percent) to upgrade security. Other reasons cited included to use staff more cost-effectively (12 percent), to reduce wear and tear on the alarm system (4 percent), or to comply with a central office mandate (4 percent). In nine out of ten cases, the equipment did the job for which it was purchased. When the technology failed, the major reasons given were:

- The sensors didn’t work properly,
- The sensors were shut off, or
- The system did not interface properly with other equipment because of poor design and installation.

Bugs. Sixty-nine percent of the sample facilities reported experiencing post-installation problems; for nine institutions the debugging process lasted years. For the sample facilities the average time to debug was 16.4 months (ranging from 5 days to 8 years). In one out of four cases (27 percent), the system never was successfully debugged. And three out of ten respondents had to spend additional funds on the debugging.

ACCESS-CONTROL SYSTEMS

Access-control system technology is relatively new in corrections. The average age of access-control systems in sample the institutions was 4 years (ranging from 1 to 14 years).

In general, two approaches were used to control access into secured areas: push-button code and card-access systems. Push-button code systems were preferred by 41 percent of the 17 sample facilities that had access-control systems. Card-access systems accounted for another 30 percent, while the remaining 29 percent had chosen among electrical lock override systems, audio identification systems, and door and gate control panels.

All facilities that had an access-control system listed a specific reasons for installing it, including:

- To limit access to doors and certain areas,
- To reduce the number of keys,
- To have a permanent printed log of access,
- To provide after-hours access to the segregation unit and to the medical department,
- To provide easy access by emergency personnel,
- To eliminate the hassle of rekeying doors (changing access codes was easier), and
- To monitor inmate movement.

For eight out of ten facilities, the access-control equipment solved the problem for which it was installed, in the others, the difficulty was not resolved because the equipment was not installed properly, repairs were not made promptly, or there were too many breakdowns or false alarms.

Eighty-six percent of the respondents indicated that access-control systems were essential to their facilities’ security. Had they ***not*** been installed, more staff would have been needed to ensure outside door security, additional security locks would have been installed requiring more keys, and there would have been no automatic record of security rounds.

Location

Table 4-11 lists the sites within correctional institutions where access-control systems were used; most frequent were clinics/infirmaries and armories (53 percent each). Additionally, the technology was used in boiler/mechanical rooms, food service areas, “bubble” and sally-port control centers, locksmith shops, computer rooms, high-security-risk tool rooms, and staff break/locker rooms.

Respondents thought access-control systems should also be used for staff access to recreation and equipment check-out rooms, administrative corridors, and mechanical service closets.

Half the institutions used their access-control systems to document and identify entry into restricted areas. Of these, 55 percent had developed methods to prevent documentation alterations.

The signal from the access-control system was usually (63 percent of the cases) both light and audio; but could be just light (19 percent) or just audio (6 percent).

Table 4-11
Placement of Access-Control Systems

	No. of Facilities	%*
Clinic/Infirmary	9	53
Weapons Room (Armory)	9	53
Officer Station/Post	8	47
Administrative Offices	5	29
Cells	4	24
Drug Dispensary	4	24
Work Areas	4	24
Commissary	2	12
Control Center	2	12
Business Office	1	6

* The total percentage exceeds 100 because a number of respondents reported that they placed their access-control systems in more than one location.

Installation and Debugging

Outside contractors were most often (78 percent of the time) used to install the access-control systems. Performance bonds were required of the installer by 83 percent of the facilities. Spare parts for this technology were reported as readily available from the manufacturer by 87 percent of the respondents; 63 percent of the facilities kept spare parts in stock themselves.

Seventy-one percent of the responding institutions had to debug their access-control technology after it was installed. For 26 percent of them, their system was never successfully debugged. Thirty-one percent of the respondents spent additional funds on the debugging.

Tampering

For 85 percent of the facilities, access-control systems were tamper-resistant as installed. Those institutions whose systems were not tamper-resistant as installed added covers to the equipment and replaced regular screws with tamper-resistant types. One out of four systems had been breached; such system failures caused by tampering allowed access to the armory, caused indicators to show improper signals, and allowed doors to be left open.

Maintenance and Repair

Half the facilities had scheduled maintenance and testing for their access-control systems. Most often this was done daily. Staff did the maintenance in 78 percent of the facilities and system testing in 22 percent. Only a third of the institutions with scheduled maintenance experienced many problems that required repairs. The most common repairs listed were wiring and replacement of malfunctioning relay driver boards and switches.

AUDIO-MONITORING SYSTEMS

Although 30 (60 percent) of the respondents had audio-monitoring systems, only 6 answered all the items in that section of the questionnaire. Consequently, the data for audio-monitors had more anecdotal than statistical validity and cannot be reported on here (see instead the Questionnaire Data section of the Appendix).

Conclusions and Issues

CONCLUSIONS

Generally, the corrections administrators who responded to the monitoring and surveillance systems survey were satisfied with their equipment. In their collective opinion, institution security would be severely compromised without it. However, help in planning for monitoring and surveillance improvements emerged as a consistent undertone in the replies received.

The most common monitoring and surveillance technology being used was closed-circuit television (CCTV) (90 percent of the sampled facilities). The average number of monitoring screens per institution was 14, each of which monitored an average of six cameras. The average number of screens monitored by one staff member was six. In all instances, these operators had additional duties (e.g., monitoring control panels, issuing keys and equipment, answering telephones, and escorting high security prisoners). In some cases, one staff member watched as many as 18 screens, and one screen switched among 10 to 50 cameras!

Clearly, to the degree that institutions approached this extreme, the use of CCTV made a mockery of its original intent. Rather than enhancing the staff's monitoring capabilities, CCTV became a technological facade, placing in jeopardy the lives of both inmates and facility personnel.

Although 78 percent of the facilities reported a desire for additional cameras, the survey data suggested the need may be less for equipment than it is for better planning, preferably based on time-motion studies.

Motion detection technology was used by 58 percent of the respondents. More than half of them (54 percent) reported equipment-caused false alarms. In addition to installation problems, reasons cited for system difficulties centered on poor design and the fact that the equipment did not interface with other monitoring and surveillance technology.

In general, the monitoring and surveillance survey data suggested there was little coordination among systems' designers, installers, and operators during the planning process.

ISSUES

General Issues-Monitoring and Surveillance Systems Technology

It is not enough to have high-tech internal surveillance systems. They are effective only when they function and when staff have been trained to use them properly.

As with most technology, the most important component in monitoring and surveillance systems is the people who use it. System planning should incorporate both a facility's security needs and staff requirements into the design process.

The task force that develops the monitoring and surveillance system should include specialized personnel who understand the problems to be solved, from both management's and users' perspectives. It can, then, review proposals in terms of those that are most appropriate. The development team should address the following:

1. Identify all facility hazards that require monitoring.

2. Determine precisely what current problems the monitoring and surveillance technology should resolve.

3. Identify potential environmental problems (e.g., lighting for CCTV or noise levels for audio-detection), and ensure that equipment will be able to avoid their detrimental effects.

4. Determine whether or not the facility has the correct wiring that the new equipment will require.

5. Determine whether or not the benefits expected from the equipment outweigh the costs of its purchase, installation, and maintenance.

6. Contact other users of the equipment to be purchased to benefit from their experience.

7. Purchase monitoring and surveillance equipment for which parts will be readily available, and will remain available, once the system is installed and for which there are local contractors who can provide 24-hour service.

8. Determine whether or not the system has a good warranty-one that is explicit as to what is covered.

9. Develop a plan for onsite support

10. Ask the vendor to provide detailed documentation of the monitoring and surveillance system.

11. Obtain schedules for maintenance and repair from the manufacturer, vendor, and/or installer and a schedule for (and information on) appropriate testing methods.

12. Determine whether or not maintenance and repair of the system will be accomplished by facility staff or by a maintenance contract.

13. Make sure the amount and type of training is specified. Sound training involving modern technology requires a long lead time; therefore, start training as early as practicable. Plan for staff to be trained in how to operate, maintain, and repair the system. Try to arrange the training as part of the sales contract.

14. Decide the level of staff that will be trained, and ensure that management as well as support staff are included.

15. Plan now on how follow-up training will be provided for both present personnel and new hires.

16. Consider whether or not the monitoring and surveillance system can be expanded to meet future needs of the facility.

Closed-Circuit Television Technology Issues

Decisions as to exactly what a new closed-circuit television (CCTV) system is to accomplish should be made before it is installed. Staffing considerations should also be built into the planning process. Absent such procedures, there is a high likelihood that CCTV's effectiveness will be seriously compromised.

Equipment. When selecting CCTV equipment, consider the available light at the locations to be monitored. Ensure that it is sufficient for the cameras to work effectively. Low light-level cameras are available, but if there is a protected lighting system, regular cameras should be adequate.

Consider installing a good zoom lens to allow close-ups of suspicious activity. For cameras installed outdoors, ensure that they are encased in all-weather housing. Some cameras may need pan-and-tilt capabilities to be able to follow suspected intrusions.

CCTV monitors are made in different sizes, shapes, and with varying capabilities. In most instances, two or more cameras will be monitored by one screen equipped with an automatic sequencing device to switch from one camera to another. Such a system should have a manual override that allows the operator to stay on one camera and use pan/tilt and zoom capabilities to zero-in on any suspicious activity.

Video tape recorders are valuable when a record is needed for later positive identification or as evidence. The operator should be able, at the touch of a button, to have a permanent visual record made of what is taking place.

In all instances, prior to purchase arrange for a field test of the equipment. The test should be conducted onsite at the location where it is to be used. This will help ensure that the technology will meet the needs of the facility.

Placement. To assist in determining the best locations for CCTV cameras, the following steps should be considered:

1. Organize a decisionmaking task force that includes representatives from management, security, and maintenance to decide where cameras should be placed.

2. Prepare a preliminary list of every location where CCTV would be helpful.

3. Determine the advantages and disadvantages of placing a camera at each of these locations.

4. Rate the locations in order of importance to an institution-wide safety and security program.

5. Determine in which of the areas on the list the cost to purchase, install, and maintain the equipment would be exceeded by the usefulness derived from the technology.

6. Remember that the entire system does not have to be installed at once. A basic system can be installed during one fiscal year with additions being made as the budget allows.

7. Consider any future expansion that might require construction (e.g., installing cable is much more economical at the time of construction than at some later time).

Training. When the installation has been completed, ensure that each staff member who will be assigned to operate the equipment receives comprehensive training by the manufacturer, vendor, and/or installer. This training should include not only how to operate the system but also ways to help ensure that the operator remains alert and ready to respond when problems are detected. Additionally, both initial and follow-up training should be planned so that ***all staff*** will know how to make the monitoring and surveillance system do what they want it to do.

Chapter 4

Questionnaire Data-Monitoring and Surveillance Systems

50 Responses

Audio-Monitors	30	Access-Control and Monitoring Systems:	
Motion Detectors	29	Card-Access	5
Closed-Circuit Television	45	Rush-Button Code	8
		Other (specify)	0

Closed-Circuit Television (CCTV)

1. When was the CCTV system installed in this facility?
   # Responses - 39　Average Age - 6 Yrs　Newest - 1 Yr　Oldest - 25 yrs
   Don't Know 5

2. Is the CCTV system essential to the security of the facility?
   Yes 36　No 8　Don't Know 0　No Response 1

3. If yes, what would be the effect on the security of the facility if the CCTV system was removed?
   (covered in text)

4. Is CCTV used to record situations when security or conduct violations may occur?
   Yes 22　No 23　Don't Know 0

5. Does the system have built-in taping capability?
   Yes 18　No 24　Don't Know 3

6. If yes, taping is started [Check (x) ONE]

Automatically	1
Manually	16
System Tapes Continually	3
No Response	25

7. Does the system have audio capabilities?
   Yes 20　No 21　Don't Know 0　No Response 4

8. What is the total number of cameras in your facility?
   # of Responses - 41　Average # of Cameras - 21　High 125　Low 1

9. What is the total number of monitoring screens in your facility?
   # of Responses - 42　Average # of Screens - 14　High 150　Low 1

10. Is there a need for additional cameras?
    Yes 32　No 9　Don't Know 0　No Response 4

11. Are monitoring screens all in one location?
Yes 16 No 28 Don’t Know 0 No Response 1

12. In what areas are the screens located? (covered in text)

13. Do some screens monitor more than one camera?
Yes 36 No 7 Don’t Know 0 No Response 2

14. If yes, what is the maximum number of cameras monitored by one screen?
# of Responses - 36 Average # of Cameras - 5.53 High 50 Low 1

15. What is the maximum number of screens monitored by one staff member at any one time?
# of Responses -41 Average # of Screens - 5.78 High 18 Low 1

16. What is the number of staff monitoring the screens on each of these shifts?

No Response - 4

<u>8:OOam - 4:OOpm</u>
# of Responses - 41
Average # of Staff - 3.12
High 32 Low 1

<u>4:OOpm - 12:OOpm</u>
# of Responses - 41
Average # of Staff - 2.93
High 30 Low 1

<u>12:OOam - 8:OOam</u>
# of Responses - 41
Average # of Staff - 2.51
High 24 Low 1

17. Do staff members who monitor screens have additional duties?
Yes 43 No 1 Don’t Know 0 No Response 1

18. If yes, what other duties do they perform? (covered in text)

19. The monitors are [Check (x) ONE]

Color	3
Monochrome	40
Both	2

20. Does lighting affect the screens?
Yes 28 No 15 Don’t Know 2

21. If yes, how are the screens affected? [Check (x) ALL that apply]

Screens are not easily visible	22
Lighting damages the screens	1
Other (specify)	7
No Response	15

22. Is the CCTV used as part of a motion detection system?
Yes 7 No 37 Don’t Know 1 No Response 0

23. Does the facility have a regularly scheduled maintenance/testing program for the CCTV system?
Yes 16 No 27 Don’t Know 0 No Response 2

24. If yes, how often is maintenance/testing performed and what does it involve?

weekly	2
Monthly	3
Quarterly	2
Semiannually	1
Annually	1
Randomly	4
Other (specify)	10

25. Who performs the scheduled maintenance/testing and what are they responsible for?

Staff	25
Safety Officer	0
Manufacturer	0
Vendor	0
Outside Contractor	4
Other (specify)	2

26. If the facility has scheduled maintenance/testing, are there many problems that require repairs?
Yes 3 No 18 Don't Know 7 No Response 17

27. What are the three most common repairs that are required? (covered in text)

28. Is the CCTV system used out of doors?
Yes 34 No 9 Don't Know 0 No Response 2

29. If yes, to what degree is outside use of the CCTV system affected by each of the factors below? [For "a" through "g" place an (x) in the appropriate column for each factor.]

	Affected	Somewhat Affected	Not Affected	Don't Know	No Response
a. Temperature	0	8	26	1	10
b. Wind	1	14	19	1	10
c. Fog	14	17	4	0	10
d. Snow and Ice	9	13	13	0	10
e. Bright Light	15	12	8	0	10
f. Darkness	12	12	10	0	11
g. Other (specify) (covered in text)	0	3	0	0	42

30. Was the CCTV system installed in this facility for a particular reason or to solve a particular problem?
Yes 36 No 4 Don't Know 3 No Response 2

31. If the system was chosen for a particular reason, what was the reason? (covered in text)

32. Has the system met expectations in terms of solving the problem?
Yes 31 No 3 Don't Know 5 NoResponse 6

33. If it did not solve the problem, why? (covered in text)

Motion Detectors

1. If this facility uses motion detectors, what types of motion detectors are used? [Check (x) ALL that apply.]

Microwave Sensor	23
Electric Field Sensor	11
Infrared Sensor	3
Thermal Sensor	1
Other (specify)	8

2. In what areas are motion detectors used? [Check (x) ALL that apply.]

Rooftops	5
Buffer zone inside perimeter fence	13
Buffer zone inside perimeter wall	2
Buffer zone between fences	7
Hallways	3
Other (specify)	19

3. Should motion detectors be used in additional areas of the facility?
Yes 8 No 16 Don't Know 7 No Response 1

4. If yes, what other areas should have motion detectors? (covered in text)

	Yes	No	Don't Know	No Response
5. Are motion detectors used in conjunction with CCTV?	12	18	0	2
6. If no, should they be used in conjunction with CCTV?	7	7	3	1
7. Are motion detectors essential to the security of the facility?	25	5	0	2

8. If yes, what would be the effect on this facility if the motion detectors were removed? (covered in text)

9. The alarm from the motion detector is a [Check (x) ONE]:

Light	0
Audio	4
Both	25
Other (specify)	6

10. The alarm from the motion detector goes to [Check (x) ONE]:

Central Control	19
Patrol	0
Both	11
Other (specify)	4

11. Does the facility have scheduled maintenance/testing for the motion detectors?
Yes 20 No 9 Don't Know 1 No Response 2

12. If yes, how often is scheduled maintenance/testing performed on the motion detector system and what does it involve? [Check (x) ALL that apply.]

weekly	6
Monthly	3
Quarterly	1
Semiannual	2
Annual	1
Other (specify)	15

13. Who performs the scheduled maintenance/testing and what are they responsible for? [Check (x) ALL that apply.]

Staff	19
Vendor	1
Safety Officer	1
Manufacturer	0
Outside Contractor	0
Other (specify)	3

14. If the facility has scheduled maintenance/testing, are there many problems that require repairs?
Yes 7 No 17 Don't Know 4 No Response 4

15. If yes, what are the three most common repairs? (covered in text)

16. Does the facility experience false alarms caused by system malfunctions?
Yes 14 No 12 Don't Know 3 No Response 3

17. If yes, how often?

Times Per Day
# of Responses - 6
Average Times Per Day - 17.83
High 50 Low 2

Times Per Week
# of Responses - 4
Average Times Per Week - 4.75
High 10 Low 3

Times Per Month
# of Responses - l
Average Times Per Month - 3
High 3 Low 3

Times Per Year
# of Responses - 2
Average Times Per Year - 5
High 5 Low 5

18. False alarms are typically due to [Check (x) ALL that apply]

Installation Problems	4
Equipment Problems	14
Other (specify)	5

19. Does the facility experience nuisance alarms resulting from natural causes such as weather or animals?
Yes 26 No 3 Don't Know 0 No Response 3

20. If yes, how often?

Times Per Day
# of Responses - 12
Average Times Per Day - 12.25
High 50 Low 1

Times Per Week
# of Responses - 6
Average Times Per Week - 7.67
High 20 Low 1

Times Per Month	Times Per Year
# of Responses - 4	# of Responses - 2
Average Times Per Month - 51	Average Times Per Year - 6.50
High 160 Low 1	High 10 Low 3

21. To what extent is the motion detector system affected by each of the following environmental factors? [For "a" through "g" place an (x) in the appropriate column.]

	Affected	Somewhat Affected	Not Affected	Don't Know	No Response
a. Animals	14	7	5	1	5
b. Ice and Snow	5	14	6	1	6
c. Wind	7	11	8	1	5
d. Hail	9	12	5	2	4
e. Blowing Debris	8	14	5	1	4
f. Lightning	4	10	7	6	5
g. Other (specify)	3	2	0	0	0

22. Were the motion detectors installed in this facility for a particular reason or to solve a specific problem?
Yes 24 No 2 Don't Know 3 No Response 3

23. If the motion detectors were installed for a particular reason, what was the reason? (covered in text)

24. Has the equipment met expectations in terms of solving the problem?
Yes 19 No 2 Don't Know 1 No Response 2

25. If it did not solve the problem, why? (covered in text)

Audio-Monitoring

1. Check which of the following areas are audio-monitored.
[Check (x) ALL that apply.]

Dorms	2
Counselors Offices	0
Visiting Rooms	1
Multiple Occupancy Cells	1
General Population Single Cells	1
Administrative Segregation	3
Disciplinary Segregation	2
Dayrooms	1
Work Areas	1
Classrooms	2
Officer Stations or Posts	2
Other (specify)	4

2. Is audio-monitoring essential to the security of the facility?
Yes 2 No 3 Don't Know 0 No Response 1

3. If yes, what would be the effect on the security of the facility if the audio-monitoring system were removed? (covered in text)

4. Are there other areas in the facility that should be included in the audio-monitoring system?
Yes 1 No 4 Don't Know 0 No Response 1

5. If yes, what are they? (covered in text)

6. Does the audio-monitoring system use a sound threshold mechanism? (i.e., it is triggered at a set decibel level)
Yes 0 No 3 Don't Know 1 No Response 2

7. Is the audio-monitoring system zoned?
Yes 3 No 1 Don't Know 0 No Response 2

8. If the system is zoned, [Check (x) ONE]:

Each zone is monitored independently	1
All zones are monitored at a central location	2
Other (explain)	0
No Response	3

9. Does the facility have scheduled maintenance/testing of the audio-monitoring system?
Yes 3 No 2 NoResponse 1

10. If yes, how often is scheduled maintenance/testing performed on the system and what does it involve? [Check (x) ALL that apply.]

weekly	1
Monthly	1
Quarterly	0
Semiannual	0
Annual	0
0ther(specify)	2

11. Who performs the scheduled maintenance/testing and what are they responsible for?

Staff	3
Safety Officer	0
Manufacturer	0
Vendor	0
Outside Contractor	0
Other (specify)	1

12. If the facility has scheduled maintenance/testing, are there many problems that require repairs?
Yes 1 No 1 Don't Know 1 No Response 3

13. What are the three most common repairs? (covered in text)

14. Was the audio-monitoring system installed in this facility for a particular reason or to solve a specific problem?
Yes 5 No 0 Don't Know 0 No Response 1

15. If the equipment was installed for a specific reason, what was that reason? (covered in text)

16. Did the equipment meet the expectations in terms of solving the problem?
Yes 4 No 0 Don't Know 0 No Response 1

17. If it did not solve the problem, why? (covered in text)

Access-Control and Monitoring Systems

1. The facility uses [Check (x) ALL that apply]:

Card-Access System	5
Rush-Button Code Access System	8

2. When was the system installed?
# Responses - 15 Average Age - 4 Yrs Oldest - 14 yrs Newest - 1 Yr
Don't Know 2 No Response 2

3. Which of the following areas have access-control and monitoring systems? [Check (x) ALL that apply.]

Weapons Room (armory)	9
Commissary	2
Business Office	1
Administrative Offices	5
Clinic/Infirmary	9
Drug Dispensary	4
Work Areas	4
Cells	4
Officer Stations/Posts	8
Other (specify)	7

4. Are there other areas that should have access-control and monitoring systems?
Yes 3 No 12 Don't Know 0 No Response 2

5. If yes, what are they? (covered in text)

		Yes	No	Don't Know	No Response
6.	Is the system used to document (record) and identify access to restricted areas?	8	8	0	1
7.	Is there a means to prevent alteration of documents?	6	5	1	5
8.	Is the system essential to the security of the facility?	12	2	1	2

9. What would be the effect on the security of this facility if the access-control and monitoring system was removed? (covered in text)

10. The alarm from the access-control and monitoring system is [Check (x) ONE]:

Light	3
Audio	1
Both	10
Other (specify)	2

11. Does the facility have scheduled maintenance/testing for the access-control and monitoring system?
Yes 7 No 7 No Response 3

12. If yes, how often is the system tested and what does it involve? [Check (x) ALL that apply.]

weekly	1
Monthly	1
Quarterly	1
Semiannual	0
Annual	0
Other (specify)	8

13. Who performs the scheduled maintenance/testing and for what are they responsible? [Check (x) ALL that apply.]

Staff	9
Vendor	0
Safety Officer	0
Manufacturer	0
Outside Contractor	1
Other (specify)	1

14. If the facility has scheduled maintenance/testing, are there many problems that require repairs?
Yes 4 No 8 Don't Know 1 No Response 4

15. What are the three most common repairs that are required? (covered in text)

16. Is the access-control and monitoring system tamper-resistant as installed?
Yes 11 No 2 Don't Know 0 No Response 4

17. If no, what measures have been taken to make it tamper-resistant? (covered in text)

18. Has the system ever been defeated?
Yes 3 No 9 Don't Know 1 No Response 4

19. Did the violations result in situations that were detrimental to the security/operation of the institution?
Yes 2 No 5 Don't Know 1 No Response 9

20. If yes, please describe the situation. (covered in text)

21. What was done to correct the problem? (covered in text)

22. Was the access-control and monitoring system installed in this facility for a particular reason or to solve a specific problem?
Yes 10 No 0 Don't Know 1 No Response 6

23. If the equipment was installed for a specific reason, what was that reason? (covered in text)

24. Has the equipment met expectations in terms of solving the problem?
Yes 8 No 2 Don't Know 0

25. If it did not solve the problem, why? (covered in text)

General Information

The following group of questions addresses general information that is applicable to each of the monitoring and surveillance systems covered in this questionnaire. As you complete this section please answer every question with a response in each of columns "A" through "D" as they correspond to the systems indicated below.

A = Closed-Circuit TV (CCTV)
B = Motion Detectors
C = Audio-Monitors
D = Access-Control and Monitoring Systems

1. Did the facility experience bugs in the system after installation was complete?

	A	B	C	D
Yes	22	18	17	15
No	16	8	11	6
Don't Know	4	2	3	1
No Response	5	19	16	25

2. If yes, for how long?

Closed-Circuit TV

Days
# of Responses - 2
Average # of Days - 4
High 5 Low 3

Weeks
# of Responses - 2
Average # of Weeks - 1.50
High 2 Low 1

Months
# of Responses - 4
Average # of Months - 6.25
High -12 Low 2

Years
# of Responses - 5
Average # of Years - 2
High 4 Low 1

Motion Detectors

Days
# of Responses - 1
Average # of Days - 5
High 5 Low 5

Weeks
# of Responses - 2
Average # of Weeks - 1
High 1 Low 1

Months
# of Responses - 3
Average # of Months - 6
High 11 Low 1

Years
# of Responses - 9
Average # of Years - 2.11
High 8 Low 1

Audio-Monitors

Days
# of Responses - 1
Average # of Days - 5
High 5 Low 5

Weeks
# of Responses - 1
Average # of Weeks - 5
High 5 Low 5

Months
# of Responses - 6
Average # of Months - 5.86
High 12 Low 1

Years
# of Responses - 4
Average # of Years - 1.75
High 3 Low 1

Access-Control and Monitoring Systems

Days
# of Responses - 0
Average # of Days - 0
High 0 Low 0

Weeks
# of Responses - 3
Average # of Weeks - 3.33
High 5 Low 2

Months
# of Responses - 3
Average # of Months - 6.33
High 12 Low 3

Years
# of Responses - 4
Average # of Years - 4
High 8 Low 2

A = Closed-Circuit TV (CCTV)
B = Motion Detectors
C = Audio-Monitors
D = Access-Control and Monitoring Systems

		A	B	C	D
3.	Was the system successfully debugged?				
	Yes	20	16	17	10
	No	7	6	5	5
	Don't Know	3	1	1	1
	No Response	17	24	24	31
4.	Were additional funds required to debug the system?				
	Yes	6	6	6	4
	No	14	14	13	9
	Don't Know	8	2	3	2
	No Response	19	25	25	32
5.	Who installed the system? [Check (x) ONE.]				
	Manufacturer	4	5	4	2
	Outside Contractor	28	22	25	14
	Staff	4	3	3	2
6.	Was the system installed according to the manufacturer's recommendations?				
	Yes	2	1	2	1
	No	0	0	0	0
	Don't Know	1	1	0	0
	No Response	44	45	45	46
7.	The specifications were written by [Check (x) ONE]:				
	Facility	1	1	1	**0**
	Consultant	1	1	1	**0**
	Vendor	0	0	0	**0**
	There were no specifications	0	0	0	**0**
	No Response	45	46	45	47

A = Closed-Circuit TV (CCTV)
B = Motion Detectors

C = Audio-Monitors
D = Access-Control and Monitoring Systems

8. Was a performance bond required of the supplier/vendor/installer?

	A	B	C	D
Yes	18	15	18	10
No	3	1	1	2
Don't Know	20	12	12	9
No Response	6	19	16	26

9. Was the supplier/vendor/installer held to the performance bond?

	A	B	C	D
Yes	0	0	0	0
No	0	0	0	0
Don't Know	3	2	2	1
No Response	44	45	45	46

10. Does the facility have an established training class in which staff learn to:

	A	B	C	D
a. Operate the system?				
Yes	0	0		
No	3	2		
b. Maintain and repair the system?				
Yes	0	0	0	0
No	3	2	2	0
No Response	44	45	45	47

11. How many hours of training are required for staff to learn to:

a. Operate the system?

CCTV
# of Responses - 2
Average # of Hours - 3.5
High 6 Low 1

Motion Detectors
# of Responses - 1
Average # of Hours - 8
High 8 Low 8

AudioMonitors
# of Responses - 2
Average # of Hours - 2
High 3 Low 1

Access-Control and Monitoring Systems
# of Responses - 0
Average # of Years - 0
High 0 Low 0

b. Maintain and repair the system?

CCTV
# of Responses - 2
Average # of Hours - 16
High 24 Low 8

Motion Detectors
# of Responses - 1
Average # of Hours - 24
High 24 Low 24

AudioMonitors
# of Responses - 2
Average # of Hours - 22
High 36 Low 8

Access-Control and Monitoring Systems
# of Responses - 0
Average # of Years - 0
High 0 Low 0

12. How many staff members are trained to:

a. Operate the system?

CCTV
#ofResponses-l
Average # of Staff - 10
High 10 Low 10

Motion Detectors
# of Responses - 1
Average # of Staff - 10
High 10 Low 10

Audio-Monitors
# of Responses - 1
Average # of Staff - 3
High 3 Low 3

Access-Control and Monitoring Systems
# of Responses - 0
Average # of Staff - 0
High 0 Low 0

b. Maintain and repair the system?

CCTV
# of Responses - 1
Average # of Staff - 1
High 1 Low 1

Motion Detectors
# of Responses - l
Average # of Staff - 1
High 1 Low 1

Audio-Monitors
# of Responses - 1
Average # of Staff - 1
High 1 Low 1

Access-Control and Monitoring Systems
# of Responses - 0
Average # of Staff - 0
High 0 Low 0

A = Closed-Circuit TV (CCTV)
B = Motion Detectors
C = Audio-Monitors
D = Access-Control and Monitoring Systems

	A	B	C	
13. Who is responsible for maintenance and repair of the system? [Check (x) ALL that apply.]				
Staff	2	1	2	
Manufacturer	0	**0**	0	
Outside Contractor	0	**0**	0	
14. If staff, which staff are trained to maintain and repair the system? [Check (x) ALL that apply.]				
Line Officers	**0**	**0**	1	**0**
Technicians	2	1	1	**0**
15. The training is provided by [Check (x) ONE]:				
Vendor	1	1	1	**0**
Facility	0	0	0	**0**

16. What is the average amount of down time per year for:

a. Repairs?

Closed-circuit TV

Hours
# of Responses - 0
Average # of Hours - 0
High 0 Low 0

Days
# of Responses - l
Average # of Days - 30
High 30 Low 30

Weeks
# of Responses - l
Average # of Weeks - 2
High 2 Low 2

Months
# of Responses - 0
Average # of Months - 0
High 0 Low 0

Motion Detectors

Hours
# of Responses - 0

Days
# of Responses - 0

Weeks
# of Responses - 1
Average # of Weeks - 3
High 3 Low 3

Months
# of Responses - 0
Average # of Months - 0
High 0 Low 0

Audio-Monitors

Hours
# of Responses - 0

Days
# of Responses - 0

Weeks
# of Responses - 0

Months
# of Responses - 0

Access-Control and Monitoring Systems

Hours
# of Responses - 0
Average # of Hours - 0
High 0 Low 0

Days
# of Responses - 3
Average # of Days - 3.33
High 5 Low 2

Weeks
# of Responses - 0

Months
# of Responses - 0

b. Unscheduled maintenance

Closed-Circuit TV

Hours
# of Responses - 1
Average # of Hours - 140
High 140 Low 140

Days
# of Responses - 1
Average # of Days - 10
High 10 Low 10

Weeks
# of Responses - 0

Months
# of Responses - 0

Motion Detectors

Hours
# of Responses - 0

Days
# of Responses - 0

Weeks
# of Responses - 0

Months
# of Responses - 0

Audio-Monitors

Hours	Days
# of Responses - 0	# of Responses - 1
Average # of Hours - 0	Average # of Days - 2
High 0 Low 0	High 2 Low 2

Weeks	Months
# of Responses - 0	# of Responses - 0

Access-Control and Monitoring Systems

Hours	Days
# of Responses - 0	# of Responses - 0

Weeks	Months
# of Responses - 0	# of Responses - 0

A = Closed-Circuit TV (CCTV)
B = Motion Detectors
C = Audio-Monitors
D = Access-Control and Monitoring Systems

		A	B	C	D
17.	If staff now perform maintenance/ repairs, do you believe a maintenance contract would help?				
	a. For cost				
	Yes	6	4	5	3
	No	24	18	21	16
	Don’t Know	5	2	1	1
	No Response	12	23	20	27
	b. For quality of repairs				
	Yes	5	2	4	2
	No	22	17	20	14
	Don’t Know	8	4	2	2
	No Response	12			
18.	Does the facility stock spare parts for key components of the system?				
	Yes	21	17	18	12
	No	19	9	13	7
	Don’t Know	0	0	0	0
	No Response	7			
19.	Are spare parts readily available from the manufacturer				
	Yes	26	19	20	14
	No	1	0	2	2
	Don’t Know	0	0	0	0
	No Response	20			

Chapter 5

Fire Safety Systems in Correctional Facilities

Abstract

Correctional Technology: A User's Guide is the product of a nationwide assessment of the experience correctional administrators have had with various types of technological systems. The purpose of this guide is to provide correctional administrators with a user-friendly source of information to aid planning and decisionmaking.

For this chapter on fire safety systems, survey questionnaires were prepared, reviewed by experts in the field of fire safety systems corrections, pilot-tested onsite, and revised in light of that input. The final version was sent to 62 correctional institutions, selected to represent all areas of the country and all levels of security. Presurvey letters and follow-up telephone calls resulted in a 100 percent response rate.

Virtually every institution in the sample (98 percent) had a smoke detection alarm system and used fire extinguishers for fire suppression. Sixty percent of the facilities experienced bugs in their fire alarm systems despite the fact that all fire system installations were made in accordance with written specifications. Once a fire safety system had been installed and debugged, system maintenance took on primary importance.

Despite some concerns, the majority of the administrators were satisfied with their fire safety systems.

Table of Contents

LIST OF TABLES

Executive Summary

Sixty-two institutions were invited to reply to the Fire Safety Systems questionnaire; all responded. These institutions were randomly distributed in terms of their security levels and geographic locations. Fifty-two percent were opened since 1980. In regard to their average daily population (ADP), there was a statistically significant relationship; the larger institutions were in the South and Midwest, and the smaller facilities were in the West.

Basically, correctional facilities in this study used two general types of fire safety equipment: alarm systems and fire suppression systems. Alarm systems activate when fire or smoke is detected, while suppression systems are used to control the spread of fires. The sample institutions had, on average, 7.7 different types of fire safety systems; the range was from 2 to 11, with 8 being the most frequent number.

For the total sample, virtually every institution (98 percent) had installed smoke detectors and some type of fire extinguishing equipment. Forty-six percent of the facilities had both ionization and photoelectric smoke detectors. The most frequently installed fire extinguisher was the combination type, which can be used for types A, B, and C fires (ordinary combustibles, flammable liquids, and electrical equipment, respectively).

Ninety-four percent of the respondents reported that their primary fire safety system had been in place an average of 10 years; in more than half the cases (53 percent) it had never been upgraded. When upgrades had been made, according to 24 of the respondents, the most frequently upgraded system involved fire suppression equipment: sprinklers 46 percent of the time, and fire extinguishers 41 percent of the time.

Overall, despite a number of concerns, most administrators (58 percent) of the sampled institutions indicated that they were satisfied with their fire safety systems.

ALARM SYSTEMS

All of the responding institutions reported having smoke detectors as part of their fire safety system. Most often facilities located these detectors in cell or dorm corridors (76 percent), offices (75 percent), dormitories (73 percent), inmate work areas (71 percent), and/or store rooms (69 percent).*

Housing unit smoke detector alarms were usually installed in the duct work (71 percent), making servicing, such as cleaning and replacement, inconvenient. Difficulties, such as false alarms, commonly resulted from humidity and/or an accumulation of dust or small insects. Humidity appeared to present more problems for institutions located in the Northeast than in other regions.

* The total percentage exceeds 100 because facilities could choose more than one response.

Ninety percent of the respondents had manual fire safety pull station alarms; the average number per facility was 50, with a range from 1 to 250. They were rarely located in housing units (8 percent), and most often were placed in work areas (78 percent), kitchens (71 percent), corridors (65 percent), and control centers (62 percent).

According to the survey data, fire safety alarm systems were least affected by thunderstorms and most negatively affected by dust and cigarette smoke. The most common repair needed was replacing batteries.

Almost three-fourths (74 percent) of the respondents had to deal with false alarms, 47 percent of which were due to equipment failure. Inmate tampering was reported as a problem by 72 percent of the institutions.

FIRE SUPPRESSION SYSTEMS

One hundred percent of the institutions surveyed had manual fire extinguishers; the average number per facility was 194, and the range was from 10 to 1,000. The extinguisher most often deployed (mentioned by 78 percent of the respondents) was the combination type, which was used for types A, B, and C fires.

Sprinkler systems were the second most prevalent fire suppression system, mentioned by 87 percent of the responding institutions. Moreover, sprinklers were most often (46 percent) listed as the most recent addition to respondents' fire safety systems. However, two-thirds of these facilities reported they did not have sprinklers in all areas. Most often, sprinklers were located in work areas (61 percent).

INSTALLATION PROBLEMS

Sixty percent of the respondents experienced bugs in their alarm systems when they were installed, despite the fact that all system installations were made in accordance with written specifications. In 77 percent of these cases, the problems were resolved at no additional cost to the facility. Requiring the supplier and/or installer to have a performance bond and then to fix any post-installation problems that developed with the system was critical to saving the costs associated with debugging. Alarm systems were significantly more susceptible to problems than were fire suppression systems-62 percent to 16 percent, in a direct comparison.

MONITORING FIRE SAFETY SYSTEMS

Once a system had been correctly installed and debugged, system maintenance became the primary concern. Alarm equipment was checked more often than suppression systems. Minimum security facilities tended to follow a weekly or monthly monitoring schedule; maximum security institutions were usually on a monthly schedule; mixed security facilities were mostly on a semiannual timetable; and, medium security institutions primarily used an annual schedule. Weekly monitoring most often consisted of a visual inspection, cleaning was primarily done on a quarterly basis, and equipment testing tended to be a semiannual activity.

Introduction

Fire is a frightening word anywhere, but particularly in correctional institutions. The normal dangers of fire and smoke are even more threatening here because these facilities have been designed to keep people in. The fact that 13 (20 percent) of the facilities surveyed had at least one major fire underlines the importance of an effective fire safety system. Responding administrators were cognizant of the damage a major fire could do to lives, property, and the most carefully managed budget.

Fire is a chemical reaction that requires four items being present in the proper ratio: fuel, oxygen (in the air or in the form of an oxidizing liquid), heat, and a chain-reaction sequence to continue a reaction once it starts. To prevent a fire, fuel must be kept away from a heat source that is capable of raising the fuel temperature to its ignition point. For example, housing areas are common sites of fires not just because that is where the inmate with an intent to set a fire spends more time, but also because that is where there is fuel for accidental as well as intentional fires. Cigarette smoking is an obvious danger, as are electrical appliances that may overload circuits. Potential for fires is also increased by accumulation by inmates of clothing, newspapers, books, other types of reading material, and hobby and craft supplies.

Fires that start in inmate housing areas pose a variety of problems for institution administrators. Some problems result from panic. Other problems can be attributed to a lack of administrative forethought (for instance, the failure to have areas of secure refuge to which inmates can be evacuated without the possibility of escape).

Fires are often started intentionally by inmates, as a show of determination during a riot situation, or as a diversion to cover an escape, to create damage as a protest against conditions, to disrupt prison operations, to injure another inmate, or to commit suicide.

Responding institutions were particularly aware of the need to control fuel load in housing units; 97 percent of the facilities had some limitations, and in 96 percent of these cases the policies were written, though one facility noted that there was poor compliance with its written policy. Methods to limit the amount of material permitted in a cell included allowing only materials issued by the state, relating the amount allowed to the inmate’s security level, and, most often, limiting the amount to that which will fit into an assigned locker or box.

An institution need not be a century old to have an archaic locking system that can hinder fire fighters’ progress. When doors open with keys only, those keys may be lost, they may break, and it is not unheard of for inmates to stuff paper and other objects into keyholes. Where doors are operated by an electrical system, as in two-thirds of the responding facilities, if the electricity goes out, the doors are inoperable unless there is a mechanical override. The default situation for an electrical system is sometimes manual operation, with the same problems as other keyed systems. Some electrical systems operate from a control center, others from within each unit. The two do not always work well together.

Even when a facility's locking systems are responsive, unless the local fire department works closely with fire safety professionals at the institution before a fire, fire fighters will not be familiar with the onsite systems or routes available for speedy and effective evacuation. Most of the responding institutions (93 percent) had agreements with local fire departments, but the terms of these varied greatly.

Buildings that lack warning or automatic suppression systems allow heat transfer, thus allowing the fire to spread through conduction, convection, and radiation. Time to escape is important. It is increased by well-constructed buildings, automatic fire protection systems, early warning through the use of automatic detection and alarm systems, and sufficient exits.

In some facilities fire safety systems were regularly tested, but few staff had been trained to use them; in others, personnel were well-trained, but testing schedules were infrequent. Sometimes it was not clear whose responsibility it was to maintain the systems, and in some cases the attempt to make a system tamper-proof made it harder to maintain.

All those who responded to this survey were acutely aware of the special problems entailed in providing fire safety in correctional facilities. The most obvious of these was that the systems that kept inmates in could also keep emergency help out.

The objective of this chapter is to provide corrections administrators with information relevant to decisionmaking about fire safety systems technology. It includes the following:

- A description, in nontechnical terms, of the types of technology in use;
- An indication of support systems and staff needed to install, operate, and service the various systems;
- Factors to be considered during the selection and planning for the use of technology; and
- Conditions under which particular technologies may be appropriate, reliable, effective, or efficient.

This chapter contains the following:

- An overview of fire safety systems,
- A description of the characteristics of the institutions sampled in the survey,
- An analysis of the survey findings,
- Conclusions drawn from survey results, and
- Issues to consider when evaluating a fire safety system.

Fire Safety Systems: An Overview

Among the facilities that responded to this survey, there were two basic types of fire safety systems in use-alarm and suppression systems-both with manual and automatic options.

FIRE SAFETY ALARMS

An alarm or alarm/detection system consists of a series of electrical switches installed on an electrical circuit which is used solely for the power supply of the alarm and detection components. These systems can fulfill many functions:

- To notify and warn occupants of fire or a hazardous condition (The alarm may be sounded locally in a room or in specified areas throughout an entire building, sent to the fire department, or a combination of these.);
- To close fire-related controls (e.g., fire doors or fire dampers) in order to prevent the spread of fire, heat, and/or smoke;
- To control ventilation and other air-handling systems for the purpose of containing a fire or retaining an extinguishing agent within a given area; and
- To release extinguishing agents and activate a prerelease alarm.

The simplest alarm actuation device is the manual pull station, a signaling system that requires a person to pull a lever to activate an audible alarm. It consists of a box with a cover that can be removed to gain access to a switch similar to a light switch. The switch allows an electrical current to flow to the warning device (e.g., an electrical bell, a horn, a siren, or a chime). It may also send a signal to the fire department, a remote fire control center, or another assistance agency. Ninety-five percent of the sampled facilities had pull systems, usually in conjunction with one or more automatic systems.

Automatic systems detect fire or smoke, and, without any human intervention, trigger an alarm signal within the premises or elsewhere. All respondents had automatic fire alarm systems that usually incorporated smoke detectors and/or heat detectors.

Smoke Detectors

The most common type of smoke detector is the photoelectric cell. Light is beamed across the detector's air chamber. When the light beam is interrupted by smoke of sufficient density, it transmits a signal to activate an alarm.

Ionization smoke detectors react to the invisible products of combustion (i.e., ions) released during the initial stages of a fire. Therefore, they are fast early-warning devices. The one drawback, unless carefully adjusted, is their sensitivity to ***any*** products of combustion (e.g., cigarette smoke).

Heat Detectors

Heat detectors are the slowest reacting of the automatic detection devices. There are two general ***types. Fixed-temperature devices*** activate an alarm when a predetermined temperature is detected. Typically, fixed-temperature detectors trigger an alarm when the surrounding temperature reaches 136 degrees Fahrenheit. ***Rate-of-rise detectors*** react to a rapid increase in temperature. Usually they activate an alarm when the temperature rises more than 15 degrees Fahrenheit per minute.

Many different types of sounding devices are used with alarm and alarm/detection systems. Their main function is to sound an alarm that will be heard clearly throughout a building despite any background noise level and will be recognized as a warning signal for evacuation.

Plans for all alarm and alarm/detection systems should be submitted to the inspection authority for approval prior to installation. After installation, the system should be tested before being accepted. Areas that should be checked, include the following:

- ***Location.*** Spacing of detectors and other activating devices should provide full coverage and should be located to respond quickly to a fire.
- ***Testing.*** The basic operating components should be tested by actual operation.
- ***Audibility.*** Sounding devices should be checked by walking though the building to determine whether or not the alarm can actually be heard. If there are dead spots where the alarm is not audible, additional devices should be installed.

FIRE SUPPRESSION SYSTEMS

A fire must not only be detected, but it must also be contained as much as possible. Most responding facilities had manual fire extinguishers (98 percent) and fire hoses (80 percent) which enabled personnel to respond promptly to a fire. Others had sprinkler systems.

Hoses most commonly used were rubber-lined and coated. Some institutions had other kinds: unlined, single-jacket rubber-lined, double-jacket rubber-lined, and hard suction-rubber. They came in two sizes: 1.5 and 2.5 inches in diameter.

Fire Extinguishers

Portable fire extinguishers were the most common suppression system reported by respondents. For their size and cost, fire extinguishers constitute an effective, economical first response to fire control. When used quickly, they are the first line of defense against fire. Therefore, staff must be properly trained in how to use the variety of extinguishers available to them.

The advantages of fire extinguishers are: (1) They are relatively simple to operate, and (2) they are portable. Their ***disadvantages*** are: (1) They must be operated manually, and (2) their effectiveness depends on the training of the person using them.

Types. In general, the responding institutions employed six different types of fire extinguishers.

- ABC (combination) extinguishers (in 87 percent of the facilities) are general-purpose devices that can be used against class A, B, or C fires (fires fed by ordinary combustibles, flammable liquids, or electrical equipment, respectively-see chart next page).

SUMMARY OF THE A, B, C, AND D'S OF FIRE EXTINGUISHERS

CLASSIFICATION SYMBOL (Label Color in Parentheses)	TYPE OF FIRE	DESCRIPTION OF MATERIALS	TYPE OF EXTINGUISHER
ORDINARY A COMBUSTIBLES (Green)	Ordinary Combustibles	Materials such as wood, paper. cloth, fiber, and many plastics.	Water, foam. aqueous film forming foam (AFFF), soda acid, multipurpose dry chemical, Halon 1211.
FLAMMABLE B LIOUIDS (Red)	Flammable Liquids	Liquids such as paint. paint thinner, gasoline. oil tar. solvents, fat. greases. and similar materials.	Dry chemical. multi-purpose dry chemical. carbon dioxide, Halon 1211.
ELECTRICAL C EQUIPMENT (Blue,	Electrical Equipment	Energized electrical equipment such as overheated fuse boxes and other electrical sources and wiring. Classification refers to source of ignition rather than to fuel as fires are classes A and B in terms of fuel.	Dry chemical. multi-purpose dry chemical, foam, AFFF. carbon dioxide. Halon 1211.
COMBUSTIBLE D METALS (Yellow)	Combustible Metals	Metals such as mag nesium titanium. zirconium. sodium-potassium alloys, and so on.	Dry powder with sodium chloride or graphite base. agents specific to particular metal hazards.

Reprinted from **"Fire Safety in Correctional Facilities: Instructor's Manual." No. SPP 69A, 1981, Page 89. Table 6.3, developed by the National Fire Protection Association under Grant No. BZ-O from the National Institute of Corrections, U.S. Department of Justice, Washington, D.C.**

- Dry chemical extinguishers (in 73 percent of facilities) and carbon dioxide extinguishers (in 58 percent of facilities) work well against flammable liquids like paint, paint thinner, gasoline, oil, tar, solvents, fats and greases, and where the source of the fire is electrical equipment, such as an overheated fuse box.
- Halon extinguishers (in 68 percent of facilities) are appropriate against fires involving ordinary combustibles, flammable liquids, or electrical equipment.
- Water extinguishers (in 67 percent of facilities) can be used when the material on fire is wood, paper, cloth, or fiber. They are also effective against some, but not all, fires involving plastics.
- Dry powder extinguishers (in 35 percent of facilities) are used to blanket combustible metals like magnesium, titanium, zirconium, and sodium-potassium alloys.
- Foam extinguishers (in 8 percent of facilities) can be used against fires involving ordinary combustibles or electrical equipment.

Ratings and Requirements. Fire extinguisher ratings are based on a standard size fire to be suppressed and the type of fire fuel to be extinguished; higher rating numbers denote greater extinguishing potential. For example, a 2A extinguisher can suppress roughly twice as much fire as a 1A extinguisher. A C-rated fire extinguisher, used for live electrical fires, has no numerical designation. Its main test is that the suppressing agent be a nonconductor of electricity. Specific information can be obtained by either examining the extinguisher's label or sending for details from the manufacturer.

Fire extinguisher requirements for any given occupancy area are determined by the inspecting authority. Several factors are considered in the selection of the proper type, capacity, and number of extinguishers required:

- Requirements of state and local fire codes (If codes do not specify requirements, National Fire Protection Association (NFPA) Standard ***No. 10-Standard for the Installation and Use of Portable Fire Extinguishers-is*** used.);
- The proper ***type*** of ***extinguishing agent*** for the hazard or hazards involved; and
- Ensuring ***sufficient capacity*** for suppressing the anticipated fire.

For example, depending upon the occupancy classification, Class A extinguishers should be located 50 to 100 feet from the hazard, while Class B fire extinguishers should be no less than 50 feet from the hazard.

Access. Visibility and access need to be considered. The longer it takes to put extinguishers into operation, the less chance there is of success in suppressing or controlling a fire. They should be placed in areas that will not become inaccessible as a result of flame and heat spread. Wherever possible, signs should be used to indicate fire extinguisher locations.

Extinguishers should be stored in cabinets or on hangers to protect them from damage. If they are hung, state or local regulations might specify height requirements. If requirements are not specified, fire extinguishers should not be hung so high that they will be inaccessible, nor so low that they will not be visible.

Training. Proper training in the use of fire extinguishers is essential for their appropriate and effective use. When training is neglected, the true value of the extinguisher as a first line of defense is nearly negated.

Inspection. Fire extinguishers should be periodically inspected and maintained. Routine field inspections cover obvious conditions. Further testing, such as hydrostatic testing (required every 5 years for most extinguishers) can only be conducted by companies or individuals with proper testing facilities. Many areas require that individuals who perform this type testing be licensed, because mixing extinguishing agents or improper recharging methods can create hazards for the person who uses the extinguisher. If there are no licensing requirements, steps should be taken to ensure that the individual or company performing the testing is qualified.

Routine inspection should include the following:

- Seeing that extinguishers are the proper type, capacity, and number and are appropriately located;
- Ensuring that fire extinguishers are visible and access is unobstructed;
- Examining for evidence of mechanical damage (e.g., dents in the container, bent control handles, cut hoses, clogged nozzles, broken gauges, etc.); and
- Determining the need for recharging by inspecting the pressure gauges, weighing the extinguisher, checking for broken wires or seals on the safety pin, or examining the service tag (or record) for date of last recharge. Fire extinguishers should be checked and recharged once each year or immediately after use.

Components. Fire extinguishers have three basic components. The first is the container which holds the extinguishing agent-water, carbon dioxide, dry chemicals, or other agents. The container's size determines how much extinguishing agent the extinguisher will hold and the size of the fire it will extinguish. The container also holds the power to expel the extinguishing agent (e.g., compressed air, chemicals, or inert compressed gas). When it is needed, an expellent moves the extinguishing agent out of the container with sufficient force to carry the agent over a distance to the seat of the fire.

Next a control cap and handle are necessary to contain the expellent and the extinguishing agent until it is needed. These vary with the type of expellent used and the operation of the extinguisher. For example, a soda-acid fire extinguisher has a cap just to keep the material in place. To put this type extinguisher into operation it is merely turned upside down. At the other end of the continuum, a carbon dioxide extinguisher requires that a handle be squeezed to release the extinguishing agent. Usually, to prevent accidental discharge, the control cap and handle have a safety pin that must be removed before the fire extinguisher can function. A wire or seal on the pin provides additional security against misuse.

The final component is the apparatus that directs the discharge of the extinguishing agent. The nature of this device depends on the design of the fire extinguisher and its extinguishing agent. A small diameter hose is used for water and water-based extinguishing agents. A fiberglass horn with a flexible, reinforced hose is used for compressed gases such as carbon dioxide and halon. A plastic nozzle with or without flexible hose is used for dry chemical extinguishers.

Automatic Sprinkler Systems

Automatic sprinkler systems have been in existence for over 100 years; they are a valuable fire loss prevention tool. These systems automatically trigger an alarm when they detect the presence of fire and begin to control its spread. Foam systems, which are common in kitchens, blanket the fire with aqueous film-forming foam.

Sprinkler systems apply water when they detect the presence of fire. Several types of sprinkler systems were reported by the responding facilities:

- Wet pipe systems contain water under constant pressure at all times throughout the system. It is the quickest acting because of the immediate availability of water. Each individual head reacts to the heat from a fire, which melts a solder link in the sprinkler, setting the water free to flow. This is the most common type of sprinkler installation where there are no unusual conditions (e.g., freezing weather).

- Dry pipe systems contain air under pressure. The water is held at the riser behind the dry pipe valve until it is needed. The heat of the fire melts a plastic cap. As soon as the orifice of the sprinkler head is clear, the air pressure begins to drop. Pressure from the water forces it past the dry pipe valve and into the overhead pipes, which carry it to the sprinkler network in a given zone. Reaction time is slower than wet pipe systems.

- Preaction systems are a variant of dry pipe systems and include heat detectors rather than plastic sprinkler head caps. Fire activates an independent heat detection device, which in turn opens the preaction valve, which allows the water to flow into any sprinklers that have been opened by the heat of the fire.

- Deluge systems have their sprinkler heads open at all times. When a fire occurs, the heat detectors signal control devices on the riser to allow water into the system. Once the system is activated, water is discharged from all sprinkler heads throughout the entire piping system (i.e., it is not zoned).

Sprinkler systems have five basic components:

Water Supply. A sprinkler system's effectiveness rests on the amount of water it can provide to extinguish a fire. The quantity must meet maximum needs (e.g., over a prolonged period of time or with a large number of heads open at the same time). It must supply the correct pressure-typically, 15 pounds per square inch at the highest point of the system when water is not flowing.

Underground Piping. This portion of the system helps transfer water. It is a series of interconnected pipes (of the same diameter) that connects the water supply to the riser. All joints must be tight fitting and able to withstand movement caused by water pressure.

Riser. This pipe (minimum of 6 inches in diameter) is a continuation of the underground pipe system and carries water up to the overhead pipe network.

Overhead. This series of interconnected piping (of various diameters) provides water to the sprinkler heads. The length and diameter of piping used is controlled by the piping schedule found in the NFPA standard on sprinkler systems. There are also restrictions on the number of sprinkler heads that can be supplied by any one particular size of pipe. The location of piping is affected by the amount of spacing required between sprinkler heads. Overhead piping must be designed to drain (flow back to the riser) and be capable of periodic flushing. It must also have an inspector's test valve at the opposite end from the riser. Opening this valve causes water to flow through the system, thereby allowing testing of the alarms and checking for blockages.

Sprinkler Heads. Sprinkler heads are placed at designated intervals (specified by NFPA Standard No. 13) along branch lines in the overhead system (e.g., maximum distance between heads is 15 feet). The sprinkler head is secured by screwing the base of the head into the overhead piping using normal plumbing procedures.

There arc three types of sprinkler heads:

- ***Fusible*** fink-Heat from a fire causes the solder in the link to fuse. Instantly, the links separate on free-rolling ball bearings, and lever arms (with off-set centers) are thrown outward by water pressure.
- ***Bulb*** type-Expands with heat and breaks, releasing the lever.
- ***Heat-cup*** type-Heat collects and then, at a given temperature, releases the levers. The temperature at which a sprinkler head will react is very important to the effectiveness of the system. If it is below the normal ceiling temperature, it will react and cause unnecessary damage; if the temperature rating is too high, it may not react until the fire has spread beyond the area of origin.

When the design for a sprinkler system has been completed, the plans need to be checked ***before*** installation begins. This can be accomplished using ***the NFPA Handbook*** and a copy of Standard No. 13. Plans for all five parts of the sprinkler system need to be checked.

Sample Characteristics

All 62 facilities who were sent Fire Safety Systems questionnaires responded. Geographic distribution, based on Bureau of Justice Statistics boundaries, was wide: 15 sites were in the Northeast, 16 each in the South and the Midwest, 13 in the West, and 2 in Canada. Of these, 16 were minimum security, 20 medium security, 9 maximum security (long-term, difficult inmates), and 15 were mixed security (i.e., no security group exceeded two-thirds of the population). Larger institutions were in the Midwest and smaller ones in the West.

LOCATION AND SECURITY LEVELS

Table 5-1 shows the geographic distribution of respondents. Most were located in the South and Midwest (27 percent each), followed by the Northeast (25 percent), and the West (21 percent). Table 5-2 shows the levels of security of the U.S. respondents.

Statistical analysis of the data used to develop Tables 5-1 and 5-2 reveals a nonsignificant (N.S.) relationship between the number of replies in each security category and geographic location; i.e., a random distribution.*

Table 5-1
Location of Sample Facilities

Location	n	%
Northeast	15	25
South	16	27
Midwest	16	27
West	13	21
Total*	60	100

* Excludes two additional Canadian facilities that responded to this survey.

AGE OF SAMPLE FACILITIES

All 62 respondents (including the two Canadian facilities) provided the opening date for their institutions (see Table 5-3). Thirty-one (50 percent) opened since 1980.

POPULATION SIZE OF SAMPLE FACILITIES

Table 5-4 shows the size of the sample U.S. facilities by average daily population (ADP). Table 5-5 breaks out the 60 U.S. facilities by region and ADP. Table 5-4 shows that 38 percent of the total sample had an ADP over 1,000. Table 5-5 shows:

- Only 1 (6 percent) of the 16 southern facilities had an ADP fewer than 500 inmates.
- There were no mid-size facilities (500-999 ADP) in the West.

* For four security levels, , X^2 = 3.342; df=9; N.S. A comparison conducted without the mixed category yielded x^2 = 3.838; df=6; N.S.

- The 15 Northeast facilities were evenly divided among small, medium, and large ADPs (5 each).

Chi square analysis of the data used to develop Tables 5-4 and 5-5 reveals a statistically significant relationship between ADP and location (less than 1 in 1,000 that the result was due to chance alone).* Larger facilities were primarily in the South and Midwest; while smaller institutions in the sample were in the West.

Table 5-2
Security Level of Sample Facilities

security	n	%
Minimum	16	27
Medium	20	33
Maximum	9	15
Mixed*	15	25
Total†	60	100

* Inmate population was less than two-thirds in any security category.
† Excludestwo additional Canadian facilities that responded to this survey.

Table 5-3
Date Facilities Opened

	n	%
Before 1900	5	8
1900-1939	7	11
1940-1979	19	31
1980-Present	31	50
Total	62	100

* X^2 = 22.522; df=6; p < .OOl.

Table 5-4
Average Daily Population

Population	n	%
Under 500	19	32
500-999	18	30
l000+	23	38
Total*	60	100

* Excludes two Canadian facilities that responded to this survey.

Table 5-5
ADP by Region

Population	Northeast	south	Midwest	West	Total
Under 500	5	1	3	10	19
500-999	5	9	4	-	18
1000+	5	6	9	3	23
Total*	15	16	16	13	60

* Excludes two Canadian facilities that responded to this survey.

Survey Findings

Data from the 62 surveys received (100% of those sent) were analyzed. The number of different fire safety systems cited for each institution ranged from 2 to 11 with an average of 7.7. The most popular of these were fire extinguishers, automatic fire alarms, smoke detectors, pull stations, heat detectors, fire hoses, and sprinklers.

Three of the sampled institutions had relatively new primary fire safety systems: 1, 15, and 36 months old. For the 51 other institutions (94 percent of those that responded to this set of questions), the primary fire safety system had been in place an average of 10 years. More than half (53 percent) of these reported that their systems had not been upgraded in 10 years.

As shown in Table 5-6, the following five fire safety systems were used by 90 percent or more of the facilities in the sample: smoke detectors, fire extinguishers, automatic fire alarms, heat detectors, and manual fire alarm pull stations.

Table 5-6 reveals that virtually all responding facilities had smoke detectors and fire extinguishers. For their smoke detectors, 46 percent of the institutions used both ionization and photoelectric types; the most frequently installed fire extinguisher was the combination (ABC) type.

Smoke detectors were the most common automatic fire alarm systems in correctional facilities (98 percent of the respondents had them). Many institutions (90 percent) had heat detectors. Combination detectors, in which a rate-of-rise feature responds to a fast fire and the fixed-temperature feature responds to a fire that builds too gradually to be detected by the rate-of-rise detector, were also popular.

Table 5-6
Fire Safety Systems - Usage

	No. of Facilities	%*
Smoke Detectors	59	98
Fire Extinguishers	59	98
Automatic Fire Alarms	57	95
Heat Detectors	54	90
Pull Stations	54	90
Automatic Sprinklers	52	87
Fire Hoses	48	80
Smoke Detectors (type):		
Ionization	23	38
Photoelectric	10	16
Both	28	46
Extinguishers (type):		
Combination	52	87
Dry Chemical	44	73
Halon	41	68
Water	40	67
Carbon Dioxide	35	58
Dry Powder	21	35
Foam	5	8

* The total percentage exceeds 100 because a number of institutions reported that they use more than one type of fire safety system.

Twenty-four of the respondents reported 72 fire safety system upgrades since the opening of their facility. The most frequent of these involved fire suppression systems (52 percent), followed by detection (28 percent), and alarm (21 percent) system additions/upgrades (see Table 5-7).

The top of Table 5-7 displays data for ***all*** the additions reported [e.g., 37 (52 percent) of the sampled facilities reported upgrading their fire suppression systems; of these, 17 (46 percent) involved sprinkler systems]. The bottom of Table 5-7 shows the 28 ***most recent*** additions, revealing the same overall pattern.

Table 5-7
Additions and Upgrades to Fire Safety Systems

	No.	%*
ALL		
* Suppression Systems	37	52
Sprinklers	17	46
Fire Extinguishers	15	41
- Dry	4	27
- Foam	2	13
- Wet	2	13
- Halon	1	7
- Unspecified	6	40
Stand Pipe/Hose	5	14
* Detection Systems	20	28
Smoke	15	75
Heat	5	25
* Alarm Systems	15	21
Pull	6	40
Central Monitor	3	20
Annunciator	2	13
Automatic	2	13
In-Duct Placement	1	7
Protecto-Wire	1	7
MOST RECENT		
* Suppression Systems	12	43
Sprinklers	7	58
Fire Extinguishers	5	42
- Dry	2	40
- Foam	2	40
- Halon	1	20
* Detection Systems	11	39
Smoke	8	73
Heat	3	27
* Alarm Systems	5	18
Pull	2	40
Automatic	2	40
Central Monitor	1	20

*** The total percentage exceeds 100 because a number of institutions reported more than one addition and/or upgrade to their fire safety systems.**

FIRE ALARM SYSTEMS

In all the responding institutions, smoke detectors were part of their fire alarm systems. Close to half the facilities (46 percent) had both ionization and photoelectric detectors. In the rest, ionization detectors (38 percent) outnumbered photoelectric detectors (16 percent) by more than 100 percent.

Smoke detectors most often were located in cell or dorm corridors (76 percent) and offices (75 percent), closely followed by dormitories (73 percent), inmate work areas (71 percent), and storage rooms (69 percent). They were less likely to be found in cells (42 percent). When smoke detectors did monitor cells, the average number they covered was 17 (range was from 50 to a low of 1). Similarly, in dormitories they might monitor as many as 16 (average was 6 and low was 1).

Housing unit smoke detectors were usually installed in the duct work (71 percent). However, this was sometimes a problem, because smoke detectors are very sensitive to dust, cigarette smoke, and steam. Susceptibility to heat and humidity problems varied with geography: Facilities in the Northeast had more problems (43 percent) than those in the Midwest (14 percent) or the West (7 percent).

Smoke detectors installed in ducts were difficult to clean, service, and repair because they were not easily accessible. In addition, the effectiveness of the detectors decreased as the number of cells or dorms each monitored increased. One facility, where duct-installed smoke detectors monitored up to 48 cells, reported problems with stopping false alarms when inmates blew smoke into the air ducts.

There was no question of the importance of smoke detectors. At least two of the major fires reported occurred in areas where no smoke detectors were operative.

While 90 percent of the institutions reported having pull stations, the average number per facility was 50 (the number ranged from 1 to 250). Pull stations were mostly located in work areas (78 percent) and kitchens (71 percent). They were common in corridors (65 percent) and control centers (62 percent), but rare in housing units (8 percent), where reliance was on smoke detectors in cells (42 percent) and dormitories (76 percent).

Virtually all facility fire alarm systems were zoned (98 percent), which suggests that deluge systems were rare in correctional facilities. Zoning was usually by housing units (80 percent) or buildings (79 percent), and often was defined by work areas (63 percent) or floors (61 percent). In a few cases zoning was by modular unit or wing.

Alarm systems could usually be reset from the control center (75 percent), though a few had to be reset from the fire department (2 percent), the chief engineer's office, or from the mechanical, electrical, or maintenance room of each building. Occasionally the system had to be manually reset zone by zone.

FIRE SUPPRESSION SYSTEMS

The one suppression system that appeared to be universal was the manual fire extinguisher. The number of extinguishers available in any one institution ranged from 10 to 1,000; the average number was 194. A few facilities (8 percent) indicated they should have more extinguishers on hand (requests ranged up to 750 and averaged 79), but most facilities were satisfied with this aspect of their fire safety systems.

In 98 percent of the reporting institutions, the type and location of extinguishers complied with the demands of local fire codes. Extinguishers deployed were most likely to be ABC combination type (87 percent of the respondents), though dry chemical (73 percent), halon (68 percent), and water (67 percent) types were also common.

Extinguishers were usually available to both inmates and personnel (in 88 percent of the facilities), although the staff were more likely to be trained in their proper use. Fifty-two (84 percent) of the facilities that responded trained their staff for an average of 4 hours; however, staff orientation might last as long as 40 hours. Only 24 percent of the institutions trained inmates (for an average of 3 hours).

Although 87 percent of the sampled institutions had sprinklers, more than two-thirds (68 percent) reported that they did not have ***full*** sprinkler coverage. Sprinklers were most likely to be found in inmate work areas (61 percent), dorms and cell or dorm corridors (57 percent), cells (52 percent), and administrative offices (50 percent). They were also common in segregation areas (46 percent) and lock-down units (41 percent). Other areas mentioned as sprinklered included food service and program areas, medical units, laundries, and perimeter towers.

More than half the facilities (60 percent) were required by state law to have fire hoses and, in fact, 64 percent of those reporting had positioned hoses at vulnerable points.

Foam suppression systems were available in only 18 (29 percent) of the facilities reporting; they were almost invariably in the kitchen (95 percent), although a few institutions had placed them in their industries area.

Seventy percent of the institutions reporting had an active smoke exhaust system, with a high probability (63 percent) that it was operated automatically.

INSTALLATION PROBLEMS

All fire safety alarm and suppression systems reported on were installed in accordance with written specifications, usually provided by the state architect (39 percent for alarms, 30 percent for suppression systems) or an outside consultant (38 percent for both systems). However, it was not unusual for the fire marshal (23 percent alarms, 18 percent suppression systems) or someone within the facility (21 percent alarms and 18 percent suppression systems) to set the specifications.

Alarm Systems

In five facilities, the alarm systems installed did not work as expected. Often the problem was a simple matter of improper installation, but at least one problem involved finding parts for an obsolete system.

Six out of ten facilities reported bugs in their alarm systems when installed. In one institution these took 18 months to be resolved, though in most institutions the debugging took 2 to 6 months (one facility was fortunate enough to get the kinks out of its system in just a day). In 77 percent of the cases where there were problems, these were resolved at no additional cost, perhaps because eight out of ten facilities required the supplier or installer to post a performance bond; and in 86 percent of the cases, they insisted that the bonded supplier or installer be required to fix any post-installation problems.

Suppression Systems

Although few facilities (7) had installation problems with fire suppression systems, none was able to resolve the difficulty in less than 3 months. In one case, problems took 2 years to work out, usually, though, at no additional cost to the facility. A performance bond was required of the installer in 71 percent of fire suppression system installations, and that installer was required to fix any post-installation problems.

Some installation problems had less to do with bugs than with organizational issues. One administrator reported that ***"on opening, I could not get my hands on a Certificate of Flushing (for underground piping), and when the piping was indeed flushed, gravel was discharged." The*** same person recommended that ***"a new facility needs to watch for the flushing of its pipes before the suppression system is connected,"*** and also suggested that a staff member monitor the installation of all systems: ***"Had a staff member been onsite and conducted a simple soap and water leak test, CO, systems would have been properly installed and would not have had to be corrected later."***

Another suggestion was that suppliers give the institution's maintenance department a preventive maintenance schedule when the system is accepted. One administrator admonished others to test every single device before accepting it to make sure the wiring is correct and problems are detected.

OPERATIONAL PROBLEMS

Respondents indicated the resistance level their alarm systems exhibited towards six detrimental environmental conditions. The best (i.e., lowest ***"not*** affected") rates were as follows:

- Dust-21 percent not affected,
- Cigarette smoke-23 percent not affected,

- Steam-42 percent not affected,
- Humidity-51 percent not affected,
- Heat-59 percent not affected, and
- Thunderstorms-65 percent not affected.

In other words, dust and cigarette smoke presented smoke detector alarm systems in the sampled facilities with the ***most*** problems. Of the 14 institutions that used heat detector, 43 percent were in the Northeast; of these, 46 percent reported problems caused by heat and/or humidity.

Table 5-8
Fire Safety Equipment Repairs Required

	No.	%*
Detection Systems	**36**	**37**
Clean Smoke Detectors	12	33
Replace Smoke Detector Heads	8	22
Replace Defective Smoke Detector	6	16
Replace Sensors	4	12
Detectors Not Operating	4	12
Replace Heat Detectors	2	5
Alarm Systems	**31**	**32**
Battery Replacement	9	29
Electronic System Failure	6	19
Replace Annunciator Lights	4	13
Replace Pull Stations	4	13
Zone-Board Problems	4	13
Humidity-Caused Problems	2	6
Lightning-Caused Problems	2	6
Suppression Systems	**5**	**5**
Water Leaks	2	40
Sprinkler Valves	1	20
Sprinkler Alarm	1	20
Carbon Dioxide Leaks	1	20
General Problems	**25**	**26**
Inmate SabotageNandalism	7	28
Cleaning	3	12
Replace "Exit" Lights	3	12
Automatic Fire Doors	2	8
Deterioration/Age	2	8
Equipment Failure	2	8
Other	**6**	**24**

* The total percentage exceeds 100 because several institutions reported more than one kind of required fire safety equipment repairs.

Respondents listed up to three of the most common repairs that their fire safety equipment required. The 50 replies named 97 equipment-type problems (see Table 5-8). Problems with fire suppression systems were ***least*** often reported (by 5 percent of the sample institutions). Detection equipment difficulties were cited ***most*** often-by 36 (37 percent) of the respondents. In general, the majority of the fire safety equipment problems (57 percent) fell into two areas: replacing equipment components (41 percent) and cleaning (15 percent).

MONITORING-MAINTENANCE, REPAIR, AND TESTING-FIRE SAFETY SYSTEMS

All the responding facilities scheduled maintenance and testing for their fire safety systems, although timetables varied with the types of testing, facility, and system. However, no amount of testing was of any use where there was no follow-up.

In one institution where monitoring was performed by trained staff and the schedule included weekly visual checks, monthly maintenance, and activation of the systems at least quarterly, the average down-time for alarms was 1 hour per year. In another where there was no follow-up to testing, the average down-time for alarms was 1 day per year.

Fire Alarm Systems

Table 5-9 shows the frequency with which fire safety alarm equipment was serviced. Sixty facilities responded to this survey question. Of the 10 respondents who indicated weekly servicing, 50 percent were from minimum security facilities. The most frequently followed schedule was monthly (25 percent); among these, minimum and medium security institutions were represented most often (each representing 33 percent of the total). Table 5-9 data suggest a relationship between fire alarm maintenance/servicing and security level:

- Minimum-weekly or monthly,
- Medium-annually,
- Maximum-monthly, and
- Mixed-semiannually.

Table 5-9
Fire Alarm Servicing Schedule
(by No. and Security Level of Sample Facilities)

Frequency	No. of Facilities	Minimum	Medium	Maximum	Mixed*	% of Total No. of Facilities
weekly	10	5	2	2	1	17
Monthly	15	5	5	3	2	25
Quarterly	12	3	5	2	2	20
Semiannually	10	1	2	1	6	17
Annually	13	2	6	1	4	22
Total	60	16	20	9	15	100

* Inmate population was less than two-thirds in any security category.

Table 5-10 shows that type of fire alarm service tended to vary with the servicing timetable (e.g., visual inspections were most often done on a weekly basis, testing semiannually, cleaning monthly or annually, and fire drills annually).

Eighty-four percent of the responding facilities did weekly visual inspections of their alarm systems; three facilities (16 percent) tested their systems that often. Twenty-seven percent operated on a monthly maintenance schedule that included visual checks, testing, and sometimes cleaning, fire drills, and analysis of the alarm summary log for potential problems.

The quarterly alarm maintenance schedule reported by 25 institutions (20 percent) usually supplemented a weekly or monthly timetable. Twenty-four facilities (20 percent) followed annual schedules, nine of which included inspection by a fire marshal. Other formats reported were daily visual checks of alarm systems and calibration of smoke detectors every 2 years.

In most facilities (63 percent), staff did the testing and maintenance. Of the 38 facilities so reporting, 32 (84 percent) had this done by safety officers. In 16 institutions (28 percent) the fire marshal came in to test and maintain the system, in 8 facilities (14 percent) the vendor did it, and in 3 (5 percent) the manufacturer came to do it. Outside contractors checked, tested, or maintained the equipment in 19 facilities (33 percent).

Interestingly, on a separate question about who is ***supposed*** to be responsible for maintenance and repair, the response was staff (67 percent), manufacturer (15 percent), and outside contractor (57 percent).

Table 5-10
Frequency of Different Types of Alarm Maintenance

		Type of Maintenance (by % of No. of Responses for Each Frequency)				
Frequency	No.*	Visual	Test	Clean	Drills	Total
weekly	19	84	16	-	-	16
Monthly	33	58	18	12	12	27
Quarterly	25	16	40	8	36	20
Semiannually	20	20	70	10	-	17
Annually	24	4	46	12	38[†]	20
Total	121					100

* The total number of responses exceeds the number of facilities in the sample because several facilities indicated that they perform alarm maintenance on more than one schedule.

[†] Inspection performed by fire marshall.

Apparently as a result of regular testing and maintenance schedules, seven out of ten facilities reported that their alarm systems had no real problems that required repair. In the other institutions, problems were most likely to crop up with equipment and general maintenance, though three facilities also reported environmental problems and tampering.

One facility indicated that annual repairs on its fire alarm system had taken as long as a month, and another reported almost 2 months. For the 25 facilities reporting down-time in hours, the average was 16 (the range was as high as 80 hours and as low as 1). For the nine facilities reporting down-time in days, the average was 4, with a high of 12 and a low of 1.

Almost three-fourths of the facilities (74 percent) had to deal regularly with false alarms, in two of these as often as twice a day. For ten institutions, the false alarm rate was at a more reasonable twice-a-month, and for 27 facilities it was a random occurrence. A few false alarms (7 percent) were attributed to installation mistakes, and considerably more to equipment failures (47 percent). Poor maintenance, environmental factors, and tampering together accounted for 46 percent of the false alarms.

Tampering was a problem even though in more than seven out of ten institutions (72 percent) the alarm system was believed to be tamper-resistant when it was installed. Methods used to prevent tampering included alarms that required keys to activate, pull stations that had covers that required two actions to activate, and baffles inside ducts in the segregation area to redirect cigarette smoke away from the smoke detector. Such baffles, however, obviously decreased the smoke detectors' effectiveness.

Environmental factors were more difficult than tampering to control. The major problems here were dust (79 percent of facilities reported their systems were "somewhat" or "very" affected), cigarette smoke (77 percent "somewhat" or "very" affected), and steam (58 percent "somewhat" or "very" affected); other environmental factors to which alarm systems were sensitive included humidity (49 percent), heat (41 percent), thunder storms (35 percent), and an occasional influx of small insects.

Would maintenance contracts have kept the alarm systems in better repair? Most administrators responding thought not: 80 percent believed maintenance contracts would not lower the cost of repairs, and 66 percent thought they would not improve the quality of fire alarm repairs.

Fire Suppression Systems

Fire suppression equipment most often consisted of some type of fire extinguisher (see Table 5-6). Respondents indicated the presence of seven types of extinguishers (facilities could indicate more than one):

- Combination (ABC) - 87 percent,
- Dry chemical - 73 percent,
- Halon - 68 percent,
- Carbon dioxide - 58 percent,
- Water - 57 percent,
- Dry powder - 35 percent, and
- Foam - 8 percent.

The most frequently deployed fire extinguisher was the combination type, found in almost nine out of ten institutions; foam extinguishers were least often available.

Table 5-11 shows the frequency with which fire suppression equipment was serviced. Fifty-eight facilities responded to this survey item.

Table 5-11
Fire Suppression Servicing Schedule
(by No. and Security Level of Sample Facilities)

Frequency	No. of Facilities*	Minimum	Medium	Maximum	Mixed[†]	% of Total No. of Facilities
weekly	11	2	5	1	3	19
Monthly	14	5	4	1	4	24
Quarterly	10	4	2	2	2	17
Semiannually	13	3	6	1	3	22
Annually	10	2	3	4	1	17
Total	58	16	20	9	13	100

* The total number excludes two Canadian facilities that responded to this survey.
[†] Inmate population was less than two-thirds in any security category.

Of the 13 responses that indicated semiannual fire suppression equipment servicing, 46 percent came from medium security institutions. Most (24 percent) facilities followed a monthly service schedule. Among these, minimum security institutions serviced their fire suppression equipment most often (33 percent of the total number of facilities who serviced monthly).

Table 5-11 also shows that fire suppression equipment was most often serviced weekly in minimum security facilities, monthly in mixed security institutions, semiannually in medium security facilities, and annually in maximum security institutions.

The type of maintenance service given fire suppression systems varied with the servicing timetable (see Table 5-12). That is, visual inspections were most often done weekly; while testing was usually performed on a quarterly or annual basis.

Table 5-12
Frequency of Different Types of Fire Suppression System Maintenance

		Type of Maintenance (by % of No. of Responses for Each Frequency)				
Frequency	No.*	Visual	Test	Clean	Maintain	Total
weekly	19	100	-	-	-	19
Monthly	26	85	8	4	4	25
Quarterly	17	12	82	-	6	17
Semiannually	23	9	61	-	4	23
Annually	17	6	88	-	6	17
Total	102					100

* The total number of responses exceeds the number of facilities in the sample because several facilities indicated that they perform maintenance on their fire suppression systems on more than one schedule.

Virtually all facilities (98 percent) had scheduled maintenance and testing for their fire suppression systems. Nineteen percent did a weekly visual check. Twenty-five percent checked their systems monthly: most (85 percent) with a visual inspection and 8 percent with an equipment test. Fire suppression systems were most likely to be tested annually (88 percent).

As with alarm systems, monitoring of fire suppression systems was most often (50 percent) assigned to the safety officer for visual inspection (76 percent) and sometimes testing (24 percent). The next most likely person to be responsible for the upkeep of these systems was an outside contractor (43 percent), who almost invariably did a full test of the system (96 percent), and was sometimes (16 percent) responsible for its maintenance.

In the 12 facilities that relied on fire marshals to monitor their systems, the marshals did testing (67 percent) as well as visual inspections (58 percent), but neither safety officers nor marshals did much maintenance themselves. In nine facilities technicians were responsible for monitoring the fire suppression systems. In two-thirds of these, the technician actually tested the equipment. Where a vendor came in regularly to check the system (ten facilities), the vendor always did a complete test, and in two out of the ten institutions the vendor also performed maintenance as well as a visual inspection. Only a few facilities arranged with the manufacturer to check their fire suppression systems.

Most institutions (87 percent) had no problems that required repairs in addition to testing, but for the few that did, their biggest concerns were cleaning, adjusting sensors and leaking valves, and adjusting flow and trouble switches. The next most common problem was condensation in compressors and clogged heads in foam systems. Occasionally a facility reported a leaking sprinkler head.

Only one in four facilities (26 percent) experienced tampering with its fire suppression systems. Common problems were pins pulled on extinguishers, broken sprinkler heads, cigarette smoke blown into detectors, fire hoses blocked with paper, and discharged fire extinguishers. Only 42 percent of facilities had to make a special effort to reduce tampering. Methods included the following:

- Key control,
- Disciplinary procedures,
- Placing control valves behind locked doors,

- Changing pull stations from glass-bar to key-operated,
- Replacing sprinklers with hoses in a high security unit,
- Locking up all systems,
- Making water valves and smoke detectors inaccessible to inmates,
- Rutting in a dry system with a time delay after a fire was detected,
- Installing tamper-proof switches on all water shut-off valves,
- Locating the suppression system in a supervised area, and
- Educating inmates about the system.

Fifty-eight percent of the administrators were satisfied with the fire safety systems they had, but 21 percent would like to see improvements. Among those suggested were interfaced systems, more areas sprinklered, a dry system, an upgrade of the present system, automatic halon, and simpler control panels. It was claimed that the suggested improvements would reduce response time (42 percent), cover more of the facility (33 percent), and generally offer better protection of life and property (25 percent). Some administrators believed that new equipment would not only give them a faster and more appropriate response to fires, but also would make it easier to get replacement parts, thus reducing down-time when their systems needed repair.

The majority of facilities stocked spare parts for key components of their fire safety systems (71 percent) and claimed that they were likely to find spare parts readily available from the manufacturer or dealer (88 percent). Most (88 percent) had architect's or engineer's drawings on hand to guide them through their system repairs.

TRAINING PATTERNS

In one facility, every member of the staff was trained in maintenance and repair of the fire, alarm system. At another institution (opened since 1980) the manufacturer of the safety system gave new staff 8 hours of training; 25 percent of the personnel had been fully trained, including the safety officer, electrician, plumber, and the maintenance supervisor. However, in 29 replies (47 percent), the average percent of staff trained to maintain and repair fire safety systems was 8 percent-the low was 1 percent. Just over half of the institutions (54 percent) required new staff be trained to work on their alarm systems. In contrast, 38 percent trained staff to work on their fire suppression systems.

Fire Alarm Systems

The staff person most likely to be trained in the maintenance and repair of fire safety alarm systems was an electrician (66 percent) or other technician (51 percent), but might also be the safety officer (20 percent) or one of several other people (32 percent), including a plumber or member of the maintenance staff.

The facility usually provided the training (52 percent), though it might also use the vendor (43 percent) or manufacturer (36 percent). Some employees were already trained when they were hired (their job description demanded it); others were trained on the job by supervisors or operations manuals.

Fire Suppression Systems

Staff trained in the maintenance and repair of fire suppression systems were more diverse: technicians (42 percent) more often than electricians (38 percent), followed by safety officers (19 percent). In addition to plumbers and maintenance staff, some facilities trained inmates to respond (under staff supervision) to fires.

About 20 percent of the reporting institutions trained staff in the maintenance and repair of suppression systems. All of these had designated training for new staff. Sometimes, the facility did the training itself (40 percent), but the vendor (40 percent) and the manufacturer (24 percent) might conduct these sessions. As with alarm systems, some facilities relied on operations manuals, on-the-job training, and the state fire marshal1 for suppression systems training.

Administrators generally agreed (79 percent) that maintenance contracts would not save them money on the cost of repairs for fire suppression systems, and 60 percent believed that a maintenance contract would not improve the quality of repairs.

Sixty-two percent of the facilities indicated they stocked spare parts for key components of their fire suppression systems, and 91 percent reported that parts were readily available from the factory or dealer. Most (85 percent) had architect's or engineer's drawings on hand.

Table 5-13 highlights results from Tables 5-9 and 5-11. It compares, by security level, the service frequency schedules for fire alarm and fire suppression systems, showing that minimum security facilities service both types of fire safety equipment ***most*** often; medium security institutions follow the ***feast*** frequent timetable.

Table 5-13
Comparison - Fire Alarm/Suppression Servicing Schedules

	Equipment System	
Type Facility	Alarm	Suppression
Minimum	Weekly/Monthly	Monthly
Medium	Annually	Semiannually
Maximum	weekly	Annually
Mixed	Annually	Monthly

Table 5-14 compares (for both fire safety alarm and suppression systems) their frequency-of-maintenance timetables for the type of service scheduled. Visual inspections of both fire safety systems were performed ***most*** frequently, while testing was conducted ***least*** often.

Table 5-14
Comparison - Fire Alarm/Suppression Maintenance Schedules

	Equipment System	
Type Maintenance	Alarm	Suppression
Visual	weekly	weekly
Test	Semiannually	Annually
Clean	Quarterly	Monthly

DIRECT COMPARISONS-ALARM VS. SUPPRESSION SYSTEMS

The survey asked respondents to directly rate both alarm and suppression systems on the same variables (facilities could list more than one area; therefore, the total percentage may exceed 100).

Table 5-15 compares alarm vs. suppression systems for bugs. A chi square analysis of frequency data was statistically significant.* That is, correctional institutions experienced a significantly greater number of problems with fire safety alarms. Differences of the proportions shown in Table 5-15 could occur by chance alone only once in 1,000 instances.

Table 5-16 shows the only other direct comparison yielding significant results: alarm vs. suppression systems in regard to presence of staff training classes for the maintenance and repair of fire safety systems. A chi square analysis of Table 5-16 frequency data was statistically significant? The differences found could occur by chance alone only once in 100 cases (i.e., correctional facilities set up a significantly greater number of training classes for maintaining fire suppression systems).

Table 5-15
Comparison - Bugs in Fire Safety Systems

	Equipment System (by % of Respondents)	
	Alarm	Suppression
Yes	62%	16%
No	38%	84%
(n)	(53)	(43)

Table 5-16
Comparison - Set-Up Staff Training Classes

	Equipment System (by % of Respondents)	
	Alarm	Suppression
Yes	30%	73%
No	70%	27%
(n)	(50)	(11)

* X^2= 20.654; df=l; p < 0.001.

† X^2 = 7.008; df=l; p < 0.01.

Table 5-17 compares locations where smoke detectors and sprinklers were most often placed (corridors and work areas, respectively). A chi square analysis yields no statistically significant results.*

Table 5-17
Comparison - Smoke Detector/
Sprinkler Locations

	Equipment System (by % of Respondents')	
Areas	Alarm: Smoke Detectors	Suppression: Sprinklers
Cells	42	52
Dorms	73	57
Corridors	76	57
Offices	75	50
Work Areas	71	61

* Total percentage exceeds 100 because a number of institutions reported more than one location for their smoke detectors and sprinklers.

Table 5-18 shows who most often was given responsibility to maintain and test fire alarm and fire suppression systems-the safety officer in both cases (no significant differences between systems were found).?

Table 5-18
Comparison - Maintenance/Testing Responsibility

	Equipment System (by % of Respondents*)	
Who	Alarm	Suppression
Fire Marshall	28	21
Manufacturer	5	5
Outside Contract	33	43
Safety Officer	55	50
Vendor	14	10

* The total percentage exceeds 100 because a number of institutions reported more than one entity was responsible for maintenance and testing.

* $X^2 = 3.025$; df=4; N.S.

† $X^2 = 1.753$; df=4; N.S.

SYSTEM ACTIVATION RESPONSES

What happened when a fire safety system was activated? Naturally, alarms were sounded, but there were also a variety of other responses: The fire prevention squad at a master control was alerted (68 percent), the air handling system shut down (68 percent), the smoke exhaust system turned on (48 percent), smoke doors (42 percent) and other doors (8 percent) were closed, alarms were sent to the fire department, and emergency exit doors were unlocked.

Two-thirds (66 percent) of the facilities had a system in place that opened some or all of their fire exits during an emergency. Typically it was operated from a central control (59 percent), though sometimes (36 percent) the control was by unit. Exits were opened manually in 15 percent of the facilities.

For 5 percent of the institutions surveyed, the alarm was sent off facility grounds, in two cases to the local fire department and in one to a 911 emergency response line. On the facility grounds, 90 percent of alarms were directed to the control center, and sometimes (18 percent) they were also sent to a remote terminal or to the institution's chief engineer.

What emergency systems were in place? All facilities had emergency generators and eight out of ten had emergency battery-pack lights, usually located to illuminate all exits. All emergency lights had been approved by local fire authorities.

Who had the authority to order a facility evacuated in a fire emergency? Usually, the designated official was the warden (88 percent), the shift commander (83 percent), or the associate warden (76 percent); less often it was the safety officer (53 percent) or a designated facility fire marshal (37 percent). Others included the highest ranking officer present and any correctional employee or staff member on the scene. Almost invariably (98 percent) a secure refuge had been designated for staff and inmates should they have to be evacuated.

Conclusions and Issues

CONCLUSIONS

In regard to fire safety, the following five types of equipment were most frequently used (90 percent or more) in correctional institutions:

- Smoke detectors,
- Fire extinguishers,
- Automatic fire alarms,
- Heat detectors, and
- Manual fire alarm pull stations.

In more than half the facilities (53 percent), the fire safety system was designed into the facility from the beginning, and in even more (56 percent) it was an integral part of the security system. Upgrading the institution was likely to mean upgrading the fire safety system (63 percent of the cases), not just because new construction offered an opportunity to design-in the system, but also as a way to bring a facility into compliance with the state codes-or a federal court order. Smoke detectors, sprinkler systems, and an automatic fire alarm were the most common upgrades made to meet state fire code requirements.

In three out of four cases, the newer fire safety systems were in addition to, rather than a substitution for, an existing technology. Where there was a substitution, most often it replaced a dry for a wet system. Additions were most likely to be smoke detectors or sprinkler systems. Eighty-five percent of responding administrators considered their new equipment more effective than the previous ones.

Training

Fewer than half the respondents (47 percent) provided data on training. Of those who did, 73 percent had fire response training for an average of 8 percent of the institution's staff; the usual amount of time spent initially was 89 hours per person. (When inmates were trained, training time averaged 148 hours per individual.)

A higher proportion of the facilities had classes that focused on suppression than on alarm systems (73 percent and 30 percent, respectively). Technicians were more likely to be given training on the fire suppression system, while electricians were the most frequent recipients of fire alarm system training.

An effort was made to keep fire safety officers up-to-date; 73 percent of the officers received specialized training in the year preceding the survey, for an average of 63 hours (the actual times reported ranged from a low of 4 hours to a high of 600). More than half the facilities (54 percent) required yearly training for their fire safety officers.

Training was conducted by the facility in about half the cases (52 percent); some (27 percent) used local fire officials (27 percent) or professionals from a nearby fire academy or university.

Cooperation with Local Fire Departments

Over half (58 percent) of the sampled institutions had their own fire response units; half of them used staff, but a few operated primarily with inmates. Almost all facilities (93 percent) had an agreement with a local fire department for assistance, and facility fire equipment was made available to community fire fighters. The remaining facilities were large enough to maintain their own fire response units, though some that were equally large had both their own units and an agreement with the local fire department.

Operational Problems

Problems reported with fire safety systems tended to be minor. Fourteen facilities had recurring trouble with smoke detectors. Inoperable detectors and detectors overly sensitive to dust and insects, as well as complications in replacing and maintaining detectors, were considered by these institutions to be equipment rather than maintenance difficulties.

Dissatisfaction with the arrangements for smoke detectors was common, particularly in the 11 facilities where the detectors were installed in the duct work. In two of these, the detectors monitored only one cell at a time; in the others, the number of cells monitored ranged from 7 to 50. There was speculation that the effectiveness of smoke detectors varied inversely with the number of cells being monitored.

Despite the fact that all fire safety systems were installed in accordance with written specifications (which, most often, were written by the state architect or an outside consultant), problems occurred. Six out of ten facilities reported bugs in their alarm systems, as installed. This was significantly higher than the 16 percent reporting difficulties with fire suppression systems.

Maintenance and Testing

Several differences in servicing schedules were found for the two fire safety systems. For alarm systems, the most frequent servicing occurred in minimum security institutions (which was also true for fire suppression systems); the most infrequent service schedule for alarms was used in medium and mixed security facilities. In contrast, the most infrequently serviced fire suppression systems were in maximum security institutions. The facility’s safety officer was most often given the responsibility for the maintenance of both systems.

Of the 33 facilities that reported monthly maintenance, 58 percent did visual inspections, 18 percent tested equipment, 12 percent cleaned, and another 12 percent performed drills.

Whether cleaning and inspection were more likely to be deferred when equipment was located in the ducts (where it was harder to reach), was not clear. What was certain was that the buildup of smoke and small insects in an ionization detector might cause false alarms by breaking the electrical current. Similar buildup in photoelectric detectors also significantly affected the intensity of light and caused false alarms.

Seventy-nine percent of the administrators believed that contracting out repairs would not save money on the cost of repairs for fire suppression systems; but 93 percent believed it would improve the quality of repairs on alarm systems.

ISSUES

In selecting fire safety systems, thought should be given to such factors as the placement of sensors (e.g., not in duct work) and a system's susceptibility to dust, cigarette smoke, and humidity.

Respondents were eager for others to learn from the problems they experienced. They provided a listing of some issues other administrators may want to think about when evaluating their own fire safety systems:

1. Ensure that all systems meet state and local fire code requirements.

2. Determine precisely what current problems the fire safety technology should resolve.

3. Determine whether or not the facility has the correct wiring that the new equipment will require.

4. Contact other users of the equipment to be purchased to benefit from their experience.

5. Purchase fire safety equipment for which parts will be readily available, and remain available, once the system is installed, and for which there are local contractors who can provide 24-hour service.

6. Determine whether or not the system has a good warranty-one that is explicit as to what is covered.

7. Ask the vendor to provide detailed documentation of the fire safety system.

8. Examine the size of the fire alarm zones. (Smaller is better--easier to localize and speed up response, and to minimize interruption of the facility's operations.) Examine the number of areas being monitored by one sensor.

9. Ensure that the various systems being installed are integrated with each other.

10. Assure that a water supply source will be available to provide the maximum amount of water needed for a prolonged period of time.

11. Check joints in underground piping systems for leaks.

12. Make sure overhead piping is installed so that it can be drained.

13. Ensure that extinguishing agents are appropriate for potential fire hazards in the facility.

14. Ensure that extinguishers have sufficient capacity to extinguish anticipated fires.

15. Make sure extinguishers are installed close to fire hazard areas.

16. Test alarm system components in situations which simulate actual operations.

17. Make sure extinguishers are visible and easy to access.

18. Determine that the alarm sounding device is loud enough to be heard above all types of background noise, displays a visual signal for hearing-impaired persons.

19. Make sure the amount and type of training is specified. Sound training involving modern technology requires a long lead time; therefore, start training as early as practicable. Plan for staff to be trained in how to operate, maintain, and repair the system. Try to arrange the training as part of the sales contract.

20. Make decisions as to who on staff should be trained to operate each system and what training schedule will be followed. Ensure that management as well as support staff are included.

21. Plan, now, on how follow-up training will be provided for both present personnel and new hires.

22. Ensure that the manufacturer will provide a maintenance contract (preferable to an independent contractor).

23. Obtain schedules for maintenance and repair from the manufacturer, vendor, and/or installer and a schedule for (and information on) appropriate testing methods.

24. Determine whether or not maintenance and repair of the system will be accomplished by facility staff or by a maintenance contract.

25. Consider whether or not the fire safety system can be expanded to meet future needs of the facility.

Chapter 5

Questionnaire Data-Fire Safety Systems

62 Responses

Pull stations	54	Foam Systems	10
Automatic Fire Alarms	57	Heat Detectors	54
Automatic Sprinkler Systems	52	Fire Hoses	48
Smoke Detectors	59	Fire Extinguishers	59
CO_2	31	Halon	32
Other (specify)	14		

		Yes	No	Don't Know	No Response
1.	The fire safety system was designed when the facility was designed.	30	27	1	4
2.	The fire safety system was installed as an integral part of the total security package.	30	24	3	
3.	Renovations/additions resulted in changes to the fire safety system of the facility.	35	21	0	

4. Describe the changes (i.e., adding a new system or retrofit). (covered in text)

5. If the facility uses more than one type of fire safety system, list them in the order in which they were installed the oldest first, the newest last. (covered in text)

6. Why was the most recent one installed?

Please answer the rest of this questionnaire based on the most recently installed fire safety systems in this facility.

7. The newest fire safety system was installed as:

An addition to the previous system	28
A ***replacement*** for the previous system	10
Don't Know	2
No Response	23

8. Is the newest fire safety system more effective than the previous system?
Yes 29 No 5 Don't Know 3 No Response 23

9. The emergency power back up is [Check (x) ONE]:
Emergency generator
Alternate source (specify) (covered in text)

		Yes	No	Don't Know	No Response
10.	Does the facility have emergency battery pack lights?	47	12	-	1
11.	Are the lights located so they provide illumination for all exits?	52	5	0	3
12.	Are the lights approved by the local fire marshal1 or authority?	51	0	5	4

13. What official(s) is/are authorized to order evacuation of all or part of the institution in a fire emergency? [Check (x) ALL that apply.]

Warden	52
Associate Warden	45
Institution Fire Marshall	22
Safety Officer	31
Shift Commander	49
Other (specify)	20
No Response	1

		Yes	No	Don't Know	No Response
14.	Are there areas of secure refuge for all staff and inmates in the event evacuation should be necessary?	57	1	0	2
15.	Is the available fuel load in the housing units controlled (e.g., are there limits on the amount of personal belongings)?	57	2	0	1

16. If yes, please describe the limits. (covered in text)

17. Does the facility have an electrical or central system to open some or all fire exits during an emergency?
Yes 23 No 20 Don't Know 0 No Response 1

18. If yes, please describe. (covered in text)

19. Is there a fire response unit onsite?
Yes 34 No 25 No Response 1

20. If yes, the fire response unit operates with [Check (x) ALL that apply]:

Staff	Inmates
# of Responses - 31	# of Responses - 17
Average - 69.35 percent	Average - 61.91 percent
High 100 Low6	High 100 Low 2.5

21. Does the facility have an established training program for the fm response unit?
Yes 32 No 12 No Response 16

22. How many hours of training are required for members of the fire response unit?

Staff	Inmates
# of Responses - 28	# of Responses - 14
Average - 89.43 Hours	Average - 147.79 Hours
High 1800 Low 4	High 1250 Low 15

23. The training for the fire response unit is provided by [Check (x) ONE]:

Facility	26
Fire Officials	15
Other (specify)	14
No Response	5

24. Has the fire safety officer received specialized training in the last year?
Yes 43 No 16 Don't Know 0 No Response 1

25. If yes, how many hours of training has the fire safety officer received in the last year?
# of Responses - 40 Average # of Hours - 62.80 High 600 Low 4

		Yes	No	Don't Know	No Response
26.	Is this training a yearly requirement?	28	24	5	3
27.	Is there an agreement with a community tire department for assistance?	54	4	0	2
28.	Is the facility fire equipment accessible to community fire fighters (e.g., do their trucks fit through sally-ports)?	53	5		

Fire Alarm Systems

1. How old is the primary fire alarm system? (If this is an estimate, please circle the answer.)

Number of Months	Number of Years
# of Responses - 3	# of Responses - 51
Average # of Months - 15	Average # of Years - 10.33
High 36 Low 1	High 100 Low 1

2. Has the primary fire alarm system been upgraded or expanded in the last 10 years?
Yes 26 No 29 Don't Know 0 No Response 5

3. Does the facility have manual pull stations?
Yes 53 No 6 No Response 1

4. If yes, how many are there?
# of Responses - 51 Average # of Manual Pull Stations - 49.67 High 250 Low 1

5. Where are the pull stations located? [Check (x) ALL that apply.]

Kitchen	39
Housing Units	44
Corridors	36
Control Center	34
Work Areas	43
Other (specify)	19
No Response	5

6. Is a smoke detector system part of the fire alarm system?
Yes 59 No 0 Don't Know 0 No Response 1

7. If yes, the smoke detectors are [Check (x) ONE]:

Ionization Detectors	22
Photoelectric Detectors	9
Both	27
Don't Know	1
No Response	1

8. Where are the smoke detectors located? [Check (x) ALL that apply.]

Cells	25
Storage Rooms	41
Dormitories	43
Cell or Dorm Corridor	45
Offices	44
Inmate Work Areas	42
Other (specify)	26

9. Are housing unit smoke detectors installed in the duct work?
Yes 42 No 17 Don't Know 0 No Response 1

10. If yes, how many cells/dorms/housing units does each smoke detector monitor?
[Give the number for all that apply.]

Don't Know 4

Cells	Dorms	Housing Units
# of Responses - 29	# of Responses - 8	# of Responses - 9
Avg # of Cells - 16.97	Avg # of Dorms - 5.63	Avg # of Housing Units - 4.89
High 50 Low 1	High 16 Low 1	High 18 Low 1

		Yes	No	Don’t Know	No Response
11.	Has this facility ever had a major fire?	12	44	3	1
12.	Have the smoke detectors ever failed to detect a major fire?	2	50	5	3

13. What happens when the alarm is set off? [Check (x) ALL that apply.]

Smoke Doors Close	25
Other Doors Close	5
Alarms Sound	56
Alert to Squad at Master Control	41
Air Handling System Shuts Down	41
Smoke Exhaust System Turns On	29
Don’t Know	0
Other (specify)	10

14. Is the fire alarm system zoned?
Yes 56 No 1 Don’t Know 0 No Response 3

15. If yes, how is it zoned? [Check (x) ALL that apply.]

Housing Units	45
Floor	34
Building	44
Work Areas	35
Other (specify)	4

16. Is the alarm sent off the facility grounds?
Yes 3 No 56 Don’t Know 0 No Response 1

17. If yes, where does it go? [Check (x) ONE.]

Local Fire Department	2
Emergency Number	1
No Response	57

18. Whom does the alarm alert on the facility grounds? [Check (x) ONE.]

Central Control	54
Remote Terminal	11
Other (specify)	22

19. Where is the reset system located? [Check (x) ONE.]

Fire Department	1
Central Control	45
Safety Office	0
Other (specify)	29

20. Does the facility have scheduled maintenance and testing for the fire alarm system?
Yes 58 No 0 Don’t Know 0 No Response 2

21. If yes, how often is scheduled maintenance and testing performed on the fire alarm system, and what does it involve? (i.e., weekly visual inspection, etc.) [Check (x) ALL that apply.]

weekly	19
Monthly	33
Quarterly	25
Semiannually	20
Annually	24
Other (specify)	9

22. Who performs the scheduled maintenance and testing and what are they responsible for? (e.g., security officer-weekly visual, etc.) [Check (x) ALL that apply.]

Staff	25
Vendor	8
Fire Marshal	16
Safety Officer	32
Manufacturer	3
Outside Contractor	19
Other (specify)	13

23. If the facility has scheduled maintenance and testing, are there many problems that require repairs?
Yes 17 No 41 Don't Know 1 No Response 1

24. What are the three most common repairs that are required? (covered in text)

25. What is the average amount of down-time per year for repairs?

Hours
# of Responses - 25
Average # of Man-hours - 15.80
High 80 Low 1

Days
# of Responses - 4
Average # of Days - 4.22
High 12 Low 1

Weeks
# of Responses - 4
Average # of Weeks - 3.25
High 8 Low 1

Months
# of Responses - 1
Average # of Months - 1
High Low

26. Does the facility experience false alarms? (alarms caused by system malfunctions)
Yes 43 No 15 Don't Know 1 No Response 1

27. If yes, how often?

Randomly 27

Per Day
# of Responses - 2
Average # Per Day - 2
High 2 Low 2

Per Week
# of Responses - 4
Average # Per Week - 2.25
High 4 Low 2

Per Month
# of Responses - 10
Average # Per Month - 2.20
High 4 Low 1

Per Year
# of Responses - 4
Average # Per Year - 5.50
High 12 Low 2

28. The false alarms are typically due to [Check (x) ALL that apply]:

Installation Problems	4
Equipment Problems	27
Other(specify)	26

29. Was the fire alarm system tamper-resistant as installed?
Yes 39 No 15 Don't Know 5 No Response 1

30. If no, what has been done to make the system tamper-resistant? (covered in text)

31. How much is the fire alarm system affected by each of the following factors?
[For "a" through "g" place an (x) in the appropriate column.]

	Not Affected	Somewhat Affected	Very Affected	Don't Know	No Response
a. Steam	22	21	9	2	6
b. Dust	12	35	9	2	2
c. Heat	30	14	7	3	6
d. Humidity	27	17	9	2	5
e. Thunder Storms	33	11	7	3	6
f. Cigarette Smoke	13	27	16	1	3
g. Other (specify)	3	2	1	2	52

32. Have you ever had a fire alarm system installed that did not work?
Yes 5 No 54 Don't Know 0 No Response 1

33. If yes, what type of system was it? (covered in text)

34. What was the nature of the problem? (covered in text)

Portable and Fixed Fire Suppression Systems

1. Is the facility fully sprinkled?
Yes 19 No 40 Don't Know 0 No Response 1

2. Where are the sprinkler heads located? [Check (x) ALL that apply.]

Cells	28
Dormitories	31
Cell or Dorm Corridors	31
Administrative Offices	27
Inmate Work Areas	33
Lockdown Units	22
Administrative Segregation	25
Other (specify)	19

	Yes	No	Don't Know	No Response
3. Do state fire regulations require that fire hoses be available?	31	21	7	I

		Yes	No	Don't Know	No Response
4.	Does the facility have fire hoses strategically placed throughout buildings?	38	21	0	1
5.	Does the facility have a foam suppression system?	17	42	-	1

6. If the facility has a foam suppression system, where is it located? [Check (x) ALL that apply.]

Kitchen	20
Serving Area	0
Other (specify)	1
No Response	39

7. Does the facility have manual fire extinguishers? Yes 59 No 0

8. How many fire extinguishers are available in this facility?
# of Responses - 58 Average # of Fire Extinguishers - 194.12 High 1000 Low 10

9. Do you believe there should be more extinguishers available?
Yes 5 No 54 Don't Know 0 No Response 1

10. If yes, how many more extinguishers do you believe this facility should have?
# of Responses - 5 Average # of Extinguishers - 79.40 High 250 Low 10

11. What type of fire extinguishers are used in this facility? [Check (x) ALL that apply.]

Water	40
Dry Chemical	44
Carbon Dioxide	35
Dry Powder	21
Combination (ARC)	52
Foam	5
Halon	41
Other (specify)	0

		Yes	No	Don't Know	No Response
12.	Are the type and location of the fire extinguishers in compliance with local fire codes?	56	1	1	2
13.	Are the fire extinguishers accessible to inmates as well as staff?	52	7	**0**	**1**
14.	Does the facility have an established training program for operation of the fire extinguishers?	54	4	**1**	**2**

15. If yes, how many hours of training are required for.

Staff	Inmates
# of Responses - 52	# of Responses - 15
Average # of Hours Annually - 3.79	Average # of Hours Annually - 2.73
High 40 Low 1	High 16 Low 1

16. Does the facility have an active smoke exhaust system?
Yes 40 No 17 Don't Know 1 No Response 1

17. If yes, the exhaust system is [Check (x) ONE]:
Manually Activated 14 Automatically Activated 24 No Response 12

18. Is regularly scheduled maintenance and testing performed on the fire suppression systems?
Yes 58 No 1 No Response 1

19. If yes, how often is scheduled maintenance and testing performed on the fire suppression systems and what does it involve? (e.g., weekly visual inspection, etc.) [Check (x) ALL that apply.]

weekly	19
Monthly	26
Quarterly	17
Semiannually	23
Annually	17
Other (specify)	4

20. Who performs the scheduled maintenance and testing and what are they responsible for? (e.g., safety officer-weekly visual, etc.)

Safety Officer	29
Fire Marshal	12
Technician	9
Vendor	10
Manufacturer	3
Outside Contractor	25
Other (specify)	9

21. If the facility has scheduled maintenance and testing, are there many problems that require repairs?
Yes 7 No 48 Don't Know 1 No Response 4

22. If yes, what are the three most common repairs that are required? (covered in text)

23. Has the facility experienced tampering with the fire suppression systems?
Yes 15 No 42 Don't Know 1 No Response 2

24. If yes, describe the nature of the tampering. (covered in text)

25. Has the facility attempted to make the fire suppression systems tamper-resistant?
Yes 22 No 31 Don't Know 2 No Response 5

26. If yes, what efforts have been made to make the systems tamper-resistant? (covered in text)

27. Is there any type of fire suppression system that you don't have that you wish you had?
Yes 12 No 45 No Response 45

28. If yes, what type? (covered in text)

29. How would this make the fire suppression system more effective? (covered in text)

30. Do you presently have any type of fire suppression system you wish you didn't have?
Yes 5 No 53 No Response 2

31. If yes, what kind? (covered in text)

32. How would the removal of this system make the fire suppression system more effective? (covered in text)

General Information

1. Did the facility experience bugs in the system after installation was completed?

	Fire Alarm Systems	Fire Suppression Systems
Yes	33	7
No	20	36
Don't Know	8	5
No Response	0	13

2. If yes, for how long?

Fire Alarm Systems	Fire Suppression Systems
Days	**Days**
# of Responses - 3	# of Responses - 0
Average # of Days - 6	Average # of Days - 0
High 10 Low 1	High 0 Low 0
Weeks	Weeks
# of Responses - 3	# of Responses - 0
Average # of Weeks - 3	Average # of Weeks - 0
High 6 Low 1	High 0 Low0
Months	Months
# of Responses - 9	# of Responses - 5
Average # of Months - 6.33	Average # of Months - 7
High 18 Low 1	High 14 Low 3
Years	Years
# of Responses - 11	# of Responses - 2
Average # of Years - 1.91	Average # of Years - 1.50
High 7 Low 1	High 2 Low1
Don't Know - 10	Don't Know - 6

3. Were additional funds required to debug the system?

	Fire Alarm Systems	Fire Suppression Systems
Yes	10	2
No	33	22
Don't Know	9	6
No Response	9	31

	Fire Alarm Systems	Fire Suppression Systems
4. Was a performance bond required of the supplier/vendor/installer?		
Yes	**29**	20
No	7	8
Don’t Know	22	18
No Response	3	17
5. Was the supplier/vendor/installer held to the performance bond?		
Yes	24	15
No	4	6
Don’t Know	26	21
No Response	7	19
6. The specifications were written by [Check (x) ALL that apply]:		
Facility	13	10
State Architect	24	18
Fire Marshal	14	11
Consultant	23	18
Vendor	4	4
There were no specifications	0	0
Don’t Know	13	0
Other (specify)	4	4
7. Who is responsible for maintenance and repair of the systems? [Check (x) ALL that apply.]		
Staff	41	25
Manufacturer	9	5
Outside Contractor	35	39
Other (specify)	2	0
8. If staff, does the facility have an established training class in which staff learn to maintain and repair the system?		
Yes	15	
No	35	
9. How many hours of training are required for staff to learn to maintain and repair the systems?		
	# of Responses - 16 Average # of Hours Annually - 31.88 High 100 Low 2	# of Responses - 7 Average # of Hours Annually - 2 1.77 High 40 Low 2

		Fire Alarm Systems	Fire Suppression Systems
10.	What percentage of staff are trained to maintain and repair the systems?		
		# of Responses - 29 Average - 7.97% High 100 Low 1	# of Responses - 13 Average - 7.46% High 25 Low 1
11.	Which employees are trained to maintain and repair the systems? [Check (x) ALL that apply.]		
	Line Officers	0	0
	Safety Officer	8	5
	Electrician	27	10
	Technicians	21	11
	Other (specify)	13	15
	No Response	20	35
12.	Is there training for any/all new staff who will be working on the systems?		
	Yes	26	14
	No	22	23
	No Response	13	24
13.	Training is provided by [Check (x) ALL that apply]:		
	Vendor	18	10
	Manufacturer	15	6
	Facility	22	10
	Other (specify)	7	7
	No Response	19	36
14.	If staff now performs maintenance and repairs, do you believe a maintenance contract would be an improvement?		
	a. For cost		
	Yes	8	6
	No	32	22
	Don't Know	5	3
	b. For quality of repairs		
	Yes	13	11
	No	25	16
	Don't Know	6	4
	No Response	17	30
15.	Does the facility stock spare parts for key components of the system?		
	Yes	42	29
	No	17	18
	No Response	17	18

	Fire Alarm Systems	Fire Suppression Systems
16. Are spare parts readily available from the factory or dealer?		
Yes	49	41
No	7	4
Don't Know	2	2
No Response	3	14

17. What is the average amount of down-time required for repairs?

Fire Alarm Systems	Fire Suppression Systems
Hours	Hours
# of Responses - 29	# of Responses - 20
Average # of Hour - 5	Average # of Hours - 6.05
High 40 Low 1	High 40 Low 1
Days	Days
# of Responses - 8	# of Responses - 4
Average # of Days - 9	Average # of Weeks - 1
High 51 Low 1	High 1 Low 1
Weeks	Weeks
# of Responses - 2	# of Responses - 0
Average # of Weeks - 4.50	Average # of Weeks - 0
High 8 Low 1	High 0 Low 0
Months	Months
# of Responses - 0	# of Responses - 0
Average # of Months - 0	Average # of Months - 0
High 0 Low 0	High 0 Low 0

	Fire Alarm Systems	Fire Suppression Systems
18. Did the architects/engineers provide as-built drawings of the systems for use by the maintenance staff!		
Yes	45	33
No	6	6
Don't Know	7	6
No Response	3	16

Chapter 6

Communication Systems in Correctional Facilities

Abstract

Correctional Technology: A User's ***Guide*** is the product of a nationwide assessment of the experience correctional administrators have had with various types of technological systems. The purpose of this guide is to provide correctional administrators with a user-friendly source of information to aid planning and decisionmaking.

For this chapter on communication systems, survey questionnaires were prepared, reviewed by experts in the field of communication systems technology, pilot-tested onsite, and revised in light of that input. The final version was sent to 69 correctional institutions selected to represent all areas of the country and all levels of security. Presurvey letters and follow-up telephone calls resulted in an 81 percent response rate.

The findings focused on four major communication approaches: telephones (found in all the sample institutions), two-way radios (in 95 percent of the facilities), intercoms (91 percent), and duress alarms (including wireless personal alarms used by 64 percent of the facilities and panic buttons used by 54 percent). The survey also found 100 percent usage of master/base stations by the respondents. As might be expected, the communications configuration used depended upon the type and mission of the facility. However, a wide-spread problem was noted in regard to the use of rechargeable nickel-cadmium (NICAD) batteries used in two-way radio systems. (If the batteries were recharged before they were totally depleted, their subsequent available charge was reduced to the amount that had been used previously, in what was termed the "memory effect.")

Table of Contents

LIST OF TABLES

Executive Summary

Security and the safety of staff and inmates are essential to effective correctional institutions. These, in turn, rely on efficient communication channels. Without the latter, you cannot achieve the former.

Communication systems transfer information. They are most critical in time of emergency. Reliable methods for communicating among staff members and between personnel and inmates helps resolve situations that, on occasion, are literally of a life-or-death nature.

Correctional administrators, planners, and fiscal officers are faced with many choices when acquiring or upgrading communication systems for new or existing institutions. The intent of this chapter is to provide information about the experiences of the 56 institutions which responded to a questionnaire dealing with communication systems.

The survey focused on four major communication approaches found in correctional institutions: telephones, intercoms, two-way radios, and duress alarms. All respondents (100 percent) had telephones and some type of master/substation network (usually for use with intercoms). Two-way radios (vehicular and walkie-talkies) were the next most used type of communication system reported (95 percent of the respondents). Intercoms were found in 91 percent of the sampled facilities, while 64 percent used personal duress alarms and 54 percent had panic buttons.

Telephones. Facilities had three different kinds of telephone systems. The inmate telephone system was used by prisoners to communicate with outside society. Most did not allow incoming calls but permitted outgoing collect calls. The most frequent ratio of number of inmates for one telephone was between 21:1 and 30:1. A second telephone system in use by the respondents was the system made available to visitors to the facilities with the telephones located in visiting rooms. Staff telephone systems were used for intrastaff communications and were located strategically throughout a facility.

More than half (58 percent) of the respondents mentioned features they would like to see added to their present system. Among the most frequently cited were interface with pocket-pagers, group calling, automatic call-back, a dedicated emergency phone, off-the-hook alarm capability, and an override ability to cut into calls made from selected phones. All desired features related to security rather than convenience. Overall, there appeared to be general agreement that these systems provided adequate equipment that was reliable and relatively quick to repair.

Intercom Systems. Ninety-one percent of the responding facilities reported that they had an intercom system. All were used in conjunction with master/base stations. Tampering by inmates was cited more frequently than the environment as being a problem with intercom systems.

These systems were used for various functions depending on the needs of the facility and the capabilities of the system; some of the uses reported were communication among facility staff, monitoring sounds from inmate areas, staff conferencing, duress alarms, and staff paging. Sometimes the intercom system was designed to interface with other electronic equipment such as telephones or public address systems.

Two-Way Radios. Two-way radios were almost as universal in corrections as telephones-only one facility did not use them; all but one minimum security institution considered them critical to security. Two types were in use: vehicular radios and hand-held, two-way transceivers (or walkie-talkies). Vehicular radios were usually installed in an automobile used for perimeter patrol or for other escape-related duties. Ninety-five percent of the sampled institutions reported using vehicular radios. Walkie-talkies were also used by 95 percent of the institutions responding to the questionnaire. Usually they were acquired to solve a specific problem, such as communicating critical information when telephones were not at hand, improving communications between staff members, or reducing response time in emergencies.

Duress Alarms. Duress alarms allowed corrections personnel to send a signal to a 24-hour staffed control center when an emergency occurred. Almost all duress alarm systems (94 percent) were acquired for a particular reason. Staff safety was an overriding consideration. In other cases, the systems were required by a consent decree or a union agreement. The alarms were less expensive than radios, an important factor in some jurisdictions. They also replaced radios where staff was in contact with inmates, particularly with prisons increasingly housing a large population of aggressive prisoners,

Wireless personal duress alarms were usually carried or worn by a staff member, but were sometimes part of a walkie-talkie. Usually (in 72 percent of the replies) duress alarms could be set off only manually. However, 28 percent of the institutions reported their alarms were automatically triggered when they were tilted beyond a specified angle (e.g., 30 degrees) for a given period of time. None of the personal duress alarms was location specific.

Wall-mounted panic button duress alarms were used by some facilities (54 percent) to address the problem of site identification. When the button was pressed, an alarm was sent that identified the specific location of the problem (since the panic button’s location coincided with the location of the problem).

Introduction

Knowledge is power. And information is crucial to a well-run correctional facility. Knowing what is happening gives correctional facility administrators the power not only to react to problems promptly but also to anticipate and prevent them. The key to that kind of knowledge is a well-designed communication system, one based on equipment that is simple to operate and that will perform continuously even while its components are being maintained and updated.

A good communication system gives staff members the information they need, when they need it, to coordinate their activities. It increases their ability to avoid inmate attempts at manipulation. And it gives staff a sense of personal security that is invaluable in lowering stress and increasing efficiency.

A good communication system must anticipate the possibility that something might go wrong. In other words, it must be customized to meet the unique characteristics of a single site. In no facility is it possible to keep all the inhabitants, both inmates and staff, in sight at all times, or even much of the time. Consequently, personnel must rely on communications technology to maintain contact.

Additionally, communication systems must be flexible enough to meet changing conditions, because in many institutions the mission and the demographics of the population change after the facility has opened. Moreover, no one ever has enough staff. Shrinking budgets require reductions in operational costs, and this, in turn, almost inevitably leads to a higher inmate-to-staff ratio. At the same time, the character of the inmates is changing. Not only are there more of them, but they appear to be more aggressive.

All these factors make the need for instantaneous communication imperative, preferably while maintaining an ability to convey as much information as possible.

The objective of this chapter is to provide corrections administrators with information relevant to decisionmaking about communication systems technology. It includes the following:

- A description, in nontechnical terms, of the types of technology in use;
- An indication of support systems and staff needed to install, operate, and service the various systems;
- Factors to be considered during the selection and planning for the use of technology; and
- Conditions under which particular technologies may be appropriate, reliable, effective, or efficient.

This chapter contains the following:

- An overview of communication systems,
- A description of the characteristics of the institutions sampled in the survey,
- An analysis of the survey findings,
- Conclusions drawn from survey results, and
- Issues to consider when evaluating a communication system.

Communication Systems: An Overview

Communication systems provide a channel by which staff members in and around a facility keep in touch with each other. The most commonly used systems are telephones, intercoms, radios (vehicular, walkie-talkies), and duress alarms (wireless personal alarms and panic buttons). Master/base stations are also widely used, especially in conjunction with intercoms.

Telephones were used universally (100 percent of responding facilities) to communicate both within correctional institutions and with the world outside the facility. Telephones are instruments containing a transmitter for converting the acoustic signals of a person's voice into electrical energy, a receiver for reconverting electrical signals to acoustic sounds, and associated signaling devices for communicating with other persons using similar instruments connected to a network. The term also refers to the complicated system of transmission paths and switching points that are connected to the instrument. The telephone contains seven different parts:

1. **Transmitter -** converts acoustic energy into electric impulses.
2. **Receiver** - operates on the relatively low power used in the telephone circuit. It converts electric energy into sounds.
3. **Anti-sidetone network -** functions to reduce sidetone and provide equalization.
4. **Dial** - operator-generated codes that are decoded by electronic circuits at the central office to select a particular far-end station.
5. **Ringer -** an alarm that alerts the subscriber to an incoming call.
6. **Switch-hook -** contains a set of electrical contacts that interrupt the flow of current from the central office whenever the handset is on-hook. The closing of these contacts (when the handset is lifted off-hook) signals the central office that the set's user wants to initiate or answer a call.
7. **Chassis** - provides mechanical support to hold all the other parts together.

Other hardware, such as electronic memory, loud speakers, and microphones, may be added to the basic set. The telephone's original function, permitting voice communication with another person, may be enhanced to allow communication with computers, automatic reporting of emergencies, and the use of written or graphic information as the input signal.

In the responding facilities, telephones were used in three ways:

An inmate telephone system, used by prisoners to communicate with outside society, generally did not allow incoming calls (93 percent) but permitted out-going collect calls (89 percent). Some of the systems restricted calls to certain numbers (61 percent) and recorded such data as date, time, and number called (45 percent).

Twenty of the responding facilities had fraud prevention capabilities built into their phone systems. Of these, 9 limited the amount of time permitted per call, 12 blocked calls to unauthorized numbers, and 13 recorded or monitored calls.

The number of inmates per phone ranged from 5:1 to 277: 1; the most frequent ratio (reported by 16 respondents) was between 21:1 and 30:1.

Visiting room phones were available for use by visitors in the facility's visiting room. Efforts to keep this system tamper-proof were generally successful (78 percent of the replies). Like other phone systems, visiting room telephones were rarely down for repairs.

Staff telephone systems were used for intrastaff communications. Half (51 percent) of the reporting institutions had their phone system programmed with a group-call option that allowed specified numbers to be called to summon staff help during an emergency. Forty-eight percent of these systems had a feature that sounded an alarm if the phone was off the hook too long.

More than half (58 percent) of the respondents mentioned features they would like to see added to their present system. Among the most frequently cited were interface with pocket-pagers, group calling, automatic call-back, a dedicated emergency phone, off-the-hook alarm capability, and an override ability to cut into calls made from selected phones; all these upgrades related to security rather than convenience.

Intercom systems provide instant communication within a single building or a whole complex. If they are not part of the telephone system, they often serve as a backup. They may also be electronically integrated with other systems to serve as a duress alarm.

Ninety-three percent of the respondents used intercom systems. Usually the intercom system was controlled from a master or base station that was always staffed and that could communicate with all other master stations and substations. Typically, substations were located throughout the housing units or in areas remote from the control room. A substation could always receive calls from master stations and might be set up to initiate calls (like alarms) and direct them to one or more master stations.

Personal duress alarms operate by wireless signal from an unobtrusive transmitter that can be activated either manually or automatically. Personnel who are not desk-bound often wear these alarms, especially when operating outside the immediate presence of other staff members. Sixty-four percent of the responding facilities used personal duress alarms.

A panic button is another kind of duress alarm and is usually affixed to a wall in a remote location within a cell block or another area where staff members must operate it on their own. When pressed by a staff member, it sends a signal that identifies the specific site location. Panic buttons were in use by 54 percent of the responding facilities.

Vehicle radios are radio communication systems in which at least one end of the radio path terminates in equipment carried in a vehicle or on a person riding in a vehicle. It can function with one or both terminals in motion. Mobile radio is the short name for "land mobile radio service" as defined by the Federal Communications Commission.

The dispatch system is a prevalent configuration. A land-based transmitter and receiver used by a dispatcher communicates with a few (or many) mobile units within the service area. The useful coverage area of such a system typically has a range of 20 to 25 miles.

Additional, accessory-type hardware is available (e.g., push-buttons, lights, printers, and keyboards). Consequently, this technology makes it possible to deliver a message to a vehicle when the occupant is away, or the mobile unit can directly access a land computer for needed information. When security is required, it is possible to scramble voice signals as well as digital codes using microelectronic devices.

In a corrections setting, these devices are either temporarily or permanently installed in cars used to patrol the facility. Staff use them particularly when the institution employs a roving patrol around its perimeter. Ninety-five percent of the responding facilities reported using vehicular radios.

Walkie-talkies are hand-held, two-way radios that allow staff, no matter where they are, to talk with each other or with the control center. Many two-way radios can be programmed to give an alarm when a staff member has been thrown to the ground. Walkie-talkies were used by 95 percent of the responding institutions.

Sample Characteristics

LOCATION AND SECURITY LEVELS

The 56 (81 percent response rate) correctional facilities that replied to the communication systems survey represented a wide range of geographic locations as well as security levels.

Table 6-1 shows the geographic distribution of the 52 U.S. institutions that responded. Table 6-2 shows the level of security of the sample facilities. For example, 29 percent of the U.S. respondents were located in the Midwest, 25 percent in the West, and equal numbers (23 percent each) in the Northeast and South. A third of the U.S. respondents were minimum security institutions, and more than a quarter were medium security.

Table 6-1
Location of Sample Facilities

Location	n	%
Northeast	12	23
South	12	23
Midwest	15	29
west	13	25
Total*	52	100

* **Excludes three additional Canadian facilities that responded to this survey. And there was one non-response.**

Statistical analyses of the data used to develop Tables 6-1 and 6-2 reveals a non-significant (N.S.) relationship between the number of respondents in each security category and geographic location.* In other words, the distribution of security levels across the geographic locations was random.

Table 6-2
Security Level of Sample Facilities

Security Level	n	%
Minimum	17	33
Medium	14	27
Maximum	11	21
Mixed*	10	19
Total†	52	100

* **Inmate population was less than two-thirds in any security category.**

† **Excludes three additional Canadian facilities that responded to this survey. And there was one non-response.**

AGE OF SAMPLE FACILITIES

As shown in Table 6-3, most of the responding U.S. facilities were relatively new-26 (50 percent) had been opened since 1980-but 9 of them were well over 50 years old.

* For the four security levels, X^2 = 6.943: df=9; N.S. A comparison conducted without the mixed category data yielded X^2 = 3.301; df=6; N.S.

Chi square analysis of the data in Table 6-3 resulted in a statistically significant finding.* In other words, a statistically significant proportion of the sampled institutions was opened recently-since 1980.

Table 6-3
Date Facilities Opened

	n	%
Before 1900	3	6
1900-1939	6	11
1940-1979	17	33
196O-present	26	50
Total*	52	100

* Excludes three additional Canadian facilities that responded to this survey. There was also one nonresponse.

POPULATION SIZE OF SAMPLE FACILITIES

Facility size by average daily population (ADP) is shown in Table 6-4. It shows that only 27 percent of the sample were large facilities with an ADP of 1,000 or more.

Table 6-5 shows the breakout of ADP by region. It shows that most of the small facilities (ADP under 500) were located in the West, most midsized (ADP of 500 to 999) were in the South, and most large facilities (ADP over 1,000) were in the Midwest.

Chi square analysis of the data used to develop Tables 6-4 and 6-5 reveals no statistically significant relationship between size of ADP and location.?

The typical U.S. institution in the sample was a minimum security facility with an ADP between 500 and 999, opened after 1980 in the Midwest.

Table 6-4
Average Daily Population

Population	n	%
Under 500	16	31
500-999	22	42
1000+	14	27
Total*	52	100

* Excludes three Canadian facilities that responded to this survey. And there was one nonresponse.

* X^2 = 17.903; df=9; p < .Ol.

† X^2 = 7.966; df=6; N.S.

Table 6-5
ADP by Region

Population	Northeast	South	Midwest	West	Total
Under 500	4	2	3	7	16
500-999	5	8	6	3	22
1000+	3	2	6	3	14
Total*	12	12	15	13	52

* Excludes three Canadian facilities that responded to this survey. And there was one non-response.

Survey Findings

Data from the 56 surveys received (81 percent of those sent) were analyzed. Respondents indicated the types of communication systems in use at their facility. The number of different devices cited for one institution ranged from 1 to 7 types; the average was 5.9, and most institutions used 6. Table 6-6 shows the frequency of usage (e.g., 100 percent of the sample facilities communicated through the use of telephones and also had master/base station networks.) Five systems were used by 91 percent or more of the sample institutions: telephones, master/base stations, vehicle radios, walkie-talkies, and intercoms.

TELEPHONES

Inmate Phone Systems

Usage. All but one facility in the sample had telephone systems for inmate use only. These systems averaged 33 phones, with a low of 1 and a high 120. The ratio of inmates-to-phones ranged from 5:1 to 277:1; the most frequently reported ratio (in 16 institutions) was between 21:1 and 30:1.

Almost all respondents (92 percent) believed the number of telephones available for prisoner use was adequate. In the seven institutions indicating a need for more phones, the average number of additional phones desired was 21 (with a low of 1 and a high of 112). Acquiring these phones would allow these facilities to approximate the survey respondents' average ratio of 25: 1.

Table 6-6
Communication Systems - Usage

	No. of Facilities	%*
Telephones	56	100
Master/Base Stations	56	100
Vehicle Radios	53	95
Wake-Talkies	53	95
Intercoms	51	91
Wireless Personal Duress Alarms	36	64
Panic Buttons	30	54

* The total percentage exceeds 100 because a number of facilities indicated that they use more than one kind of communication system.

Six out of ten facilities (61 percent) did not restrict the length of inmate calls; however 52 percent did limit calls to certain numbers. The majority of systems (89 percent) permitted out-going collect calls only, and did not allow incoming calls (93 percent). Virtually all inmate phones (94 percent) came with handsets, but only 35 percent were hearing-aid compatible.

As installed, 81 percent of the inmate telephones were tamper-proof, but 52 percent were not designed to prevent fraud. Close to half (45 percent) of the inmate telephone systems recorded such data as date, time, and/or numbers called.

Institutions were almost evenly divided regarding the monitoring of inmate calls; 56 percent did not monitor inmate calls. The responses were similar for recording inmate calls: 58 percent reported that they did not do so. Where calls were monitored, only 20 percent of facilities did it continuously, 40 percent selectively, and 40 percent randomly. In regard to recording telephone calls, the results were quite different: 59 percent recorded continuously, 29 percent selectively, and 12 percent randomly. Calls were monitored or recorded by the institution (38 and 57 percent, respectively), by the housing unit (25 and 29 percent, respectively), or by the individual inmate (29 and 14 percent, respectively).

Installation. The phones were generally supplied by a vendor (76 percent) and installed by an outside contractor (75 percent). In only one facility was the system not installed according to the manufacturer's specifications. Specifications were written by the institution (39 percent of the responding facilities), by the vendor (38 percent), or by a consultant (29 percent).

Forty-four percent of the institutions had no bugs in their telephone systems when installed. In the remaining institutions, 11 were trouble-free within 30 days, with one institution getting the bugs out in a single day. In four facilities, repairs took an average of 4 months, while in three others debugging took up to a year. In 91 percent of the institutions responding to this question, the system was successfully debugged; for 83 percent of these, the work was done without additional cost. Performance bonds were less common for phone system installations (62 percent) than for some other equipment, but where they existed, bonded installers were required to fix any post-installation problems that developed.

Maintenance and Training. Telephone systems were usually maintained and repaired by outside contractors (68 percent). Where staff did the job, there was an established training program averaging 25 hours (with a high of 40 and a low of 4 hours). Typically, maintenance and repair work was the responsibility of technicians (76 percent). Sometimes maintenance staff was trained by the vendor (67 percent of the respondents).

Phone systems were maintained and repaired relatively quickly compared with other technology. In 15 facilities the average downtime was less than 2 days, with a maximum of 5 days.

The institutions gave no endorsement for maintenance contracts. Those responding thought such contracts would reduce neither the cost (85 percent) nor improve the quality (92 percent) of repairs and maintenance. Since spare parts were reported as always (100 percent) being quickly obtainable from manufacturers, 65 percent of the responding institutions stocked no spare parts.

Visiting Room Phones

Usage. For the 18 facilities (33 percent) responding to questions about visiting room telephones, the average number of phones available was 10 (with a low of 2 and a high of 55); most (89 percent) believed the number they had was adequate. These telephones were considered tamper-proof in 78 percent of the institutions; however, they usually (65 percent) were not hearing-aid compatible.

Installation. Visiting room phones were most likely to be installed by an outside contractor (57 percent) or the facility staff (35 percent) rather than the manufacturer (8 percent). The systems tended to be designed by consultants (40 percent) or the facility (37 percent). All were installed according to the manufacturer's specifications, and in almost eight out of ten cases (77 percent), no bugs were found after installation. In the three facilities that reported some installation problems, all were cleared up within 3 days, though at some cost to the facility. A performance bond had been required by 53 percent of the institutions, but the bonded installer was required to fix post-installation problems in only 46 percent of the cases.

Maintenance and Training. Visiting room phones were generally maintained by facility personnel (75 percent). Only 29 percent of those responding had a training program for staff; they delivered an average of 39 hours of training, with a low of 8 and a high of 100 hours. Not surprisingly, technicians (78 percent) were most likely to be trained, followed by members of the maintenance department (16 percent). The training was provided by the vendor (46 percent) or the institution (39 percent).

Like other phone systems, visiting room telephones were rarely down for repairs; the average reported down-time was 7 hours. No one believed that the quality of repairs would be improved by a maintenance contract, and just one respondent thought a contract would reduce costs. Only a third of the responding facilities saw a need to stock spare parts.

Staff Phone Systems

Usage. Administrative telephone needs were served by a system available to the facility’s personnel. In only a few facilities was the staffs system interfaced with the intercom system (18 percent) or the public address system (20 percent). In another 25 percent, the staff system could be used as a site-wide intercom, while for a similar number it interfaced with pocket pagers. Almost three out of four (73 percent) institutional phones were on a PBX system, and most of those (76 percent) were memory-supported.

Slightly more than half (51 percent) of the reporting institutions had systems with a group-call option that allowed certain numbers to be called to summon staff to an emergency. Not quite half (48 percent) had a feature that sounded an alarm when a phone was off the hook too long. In close to two-thirds of the facilities (64 percent), there was a system for logging calls.

Only four out of ten replies indicated having a line monitoring system to detect faults like short circuits. In 94 percent of the facilities, a fault in one line did not affect the entire system.

Just 20 percent of the phone systems in reporting institutions were leased; the rest were purchased. Some had special features, such as an emergency alert number (24 percent), an off-the-hook alarm (32 percent), or both (44 percent).

More than half (58 percent) of those responding wanted to see their systems incorporate additional features. Their contention was that these features would allow key personnel to access the telephone system from any location and help entry-level officers to do their jobs more effectively. Features included on the wish list were:

- An interface with pocket pagers,
- Group calling,
- Automatic call-back,
- A dedicated emergency phone,
- Off-the-hook alarms,
- An override to cut into calls from selected phones,
- Cellular phones,
- A method of identifying which calls were made from which extensions, and
- Recording details of station messages.

Installation. Staff phone systems were usually installed by an outside contractor (66 percent) or the manufacturer (23 percent). Specifications for an institution’s system were provided by the facility (43 percent), a consultant (34 percent), the vendor (32 percent), or the department of corrections (14 percent). One facility provided no specifications. In all but one case, the staff telephone system was installed according to the manufacturer's specifications; 58 percent were problem-free at installation. Problems were eliminated quickly, usually within a month. In almost two-thirds (64 percent) of the facilities a performance bond was required; only one institution did not require the installer to fix post-installation problems.

Maintenance and Training. Keeping the staff telephone system up and running was usually the responsibility of an outside contractor (50 percent) or the staff (43 percent); however, only 26 percent of the respondents had a training program for phone maintenance. In those that did, the average number of hours of training was 63, with a low of 40 and high of 100 hours. Usually the staff members trained were technicians (85 percent) or members of the maintenance staff (11 percent). Most often the vendor did the training (65 percent), though 30 percent of the time the facility did its own training. Outside contractors provided this instruction in the other facilities.

Where staff did the repairs, 36 percent of the respondents thought the cost could be reduced by a maintenance contract; however, only 12 percent thought a contract would make a difference in the quality of repairs. Because spare parts were readily available from the manufacturer (90 percent), only 56 percent of the facilities kept parts in stock.

MASTER/BASE STATIONS AND INTERCOMS

Of the 56 institutions responding to the survey, 100 percent had master/base stations. For the 91 percent that reported having separate intercom systems, these master/base stations, along with numerous substations, were an integral part of that system.

Usage

Respondents reported having an average of 4 master stations within the system (ranging from 1 to 30). On average, the systems supported 39 substations, with a ratio of about 10 substations to each master station (ranging from 1 substation to 484 substations per master station).

Substations were located virtually anywhere:

- 63 percent in housing units,
- 50 percent in offices,
- 43 percent at outside entrances,
- 35 percent in sally-ports, and
- 34 percent in hallways.

Other locations included towers, classrooms, maintenance department, recreation yard, auditorium, and the hospital.

Asked where they would like to have additional substations installed, respondents suggested they would be useful between buildings, in the commissary, in the visiting room, and in all open areas available to inmates.

Usually (61 percent) substations were not accessible to inmates, but there were a significant number (39 percent) of exceptions. Two-thirds of the substations were tamper-resistant as installed.

In 90 percent of the reporting institutions, connection between the substation and master station was immediate. Sixty-nine percent of these systems allowed staff to monitor sounds from inmate areas under their jurisdiction. In only four out of ten institutions (41 percent) could some substations communicate on a conference basis.

Intercom transmission was rarely (11 percent) affected by environmental factors; the biggest problem was distance. The technology sometimes had trouble operating through steel and concrete and very occasionally, experienced problems due to wet underground lines, airborne moisture or weather conditions such as lightning.

Three out of four intercom systems (76 percent) required manual operation by staff members. Barely three out of ten facilities (29 percent) had intercom systems designed to interface with other electronic equipment, most often with telephone (67 percent) or public address systems (50 percent). Usually (71 percent) the intercom system did not function as a duress alarm. But many facilities (69 percent) could use their intercoms to page staff members in defined zones.

Installation

When intercom systems were bought, 7 percent of the institutions had no specifications, and 25 percent had criteria specified by a vendor, 34 percent by the facility itself. The greatest number (39 percent) had specifications developed by an outside consultant.

Most of the intercom systems (66 percent) were installed by outside contractors. For the remainder, installation was done by either the manufacturer or facility staff. All but one of the systems were installed according to the manufacturer's directions; nevertheless, more than half (52 percent) experienced some problems after installation. In the worst case, a system took 8 years to debug; more usually difficulties were resolved within 3 months, though one facility solved its problems within 2 days. But in 23 percent of the cases, the systems were never totally debugged.

Six out of ten facilities required a performance bond of the installer, and in two-thirds (64 percent) of these cases, they required the bonded installer to fix post-installation problems. Most often (71 percent) problems were resolved without any additional cost to the facility.

Maintenance

In a few cases (13 percent), master stations were automatically alerted (usually by a graphic display) if there was a problem within the intercom system; a problem in one area rarely (9 percent) affected the whole system.

Typically, facilities did maintenance only when there was a problem. Fewer than half (46 percent) the institutions surveyed had a scheduled maintenance and testing program for their intercom systems. One facility tested every day and another performed a daily visual check. Four facilities tested quarterly, though one did only visual testing. Two tested semiannually and one had semiannual scheduled maintenance. Four others tested randomly, one of which did regular maintenance at the same time.

Testing and maintenance were not scheduled very often, probably because intercom systems were relatively trouble-free; more than seven out of ten (71 percent) of the responding facilities reported no problems. In the remainder, the most common problems were broken switches, problems with amplifiers or wiring, and replacing circuit boards. Very rarely was a problem with vandalism reported.

For 68 percent of 31 responding facilities, intercom maintenance and equipment testing was done by staff, but sometimes supported by an outside contractor (29 percent). In other cases, the repairs were totally in the hands of the vendor or an outside contractor.

Down-time for intercom systems was generally minimal; usually problems could be resolved in a matter of hours or days. In general, intercom systems seemed relatively trouble-free. Seventy-nine percent of the facilities responding believed that maintenance contracts would not reduce the cost of repairs significantly, and 80 percent thought the quality of repairs would not be improved by a contract. Barely half (52 percent) of the facilities kept spare parts on hand for key components of their communication system, perhaps because 89 percent reported that parts were readily available from the manufacturer.

Training

Almost three-quarters (73 percent) of the facilities responding had established a maintenance training program for staff. In the eight institutions providing details of their program, the average number of hours for training was 39, with a low of 1 and a high of 100 hours.

Usually those trained were technicians (79 percent). In 46 percent of the cases, the vendor did the training, though some facilities (29 percent) also did training.

RADIOS

Usage

The responding institutions used two types of radio equipment: vehicular radios and hand-held, two-way transceivers (also known as, walkie-talkies). Both types of devices were referred to by the generic term “two-way radios.”

Vehicular radios were usually installed in an automobile used for perimeter patrol or for other escape-related duties. Ninety-five percent of the sampled institutions reported using vehicular radios.

Walkie-talkies, or hand-held radios, were also used in 95 percent of the institutions responding to the questionnaire. Usually (78 percent) they were acquired to solve a specific problem, such as communicating critical information when telephones were not at hand, improving communication between staff members, or reducing response time in emergencies.

Only one facility found that its radios did not meet expectations. They had not yet found a way to avoid signal impediments and interference from other radios.

Only three of the sampled institutions did not use two-way radios. Additionally, one that did, considered them unimportant to staff safety. All other respondents saw real dangers if two-way radios were not available:

- Staff would not be able to communicate critical information in many circumstances,
- Response time to emergencies would increase,
- Staff who did not have access to telephones would be much more vulnerable,
- Communicating with remote locations would be impossible,
- There would be a loss to perimeter security, and
- Staff on rounds would not be able to maintain contact with the control center.

In general, there was agreement among the survey respondents that two-way radios increased staff effectiveness.

The average number of hand-held radios per facility was 66 (with a low of 4 and a high of 255). In 87 percent of the institutions reporting, the total number included radios that were used for backup while others were being repaired or recharged. In all but one instance, two-way radios were used to maintain contact with officers outside as well as inside the facility.

Transmission Issues

The longest distance that two-way radios transmitted outside of an institution varied from 15 feet to 30 miles. In the 32 facilities that measured transmission range in feet, the average range was 2,677 with a high of 7,000; for the 20 institutions that measured in miles, the average range was 7 miles.

Outside Obstructions. For four out of five facilities, outside obstructions had been found to limit the range of transmission. The worst of these were other buildings and hills, both mentioned by 48 percent of the respondents. Problems for two-way radio systems were also caused by fences, electrical equipment, dense forest, metal modular units, power lines, and neighboring institutions with radios operating on the same frequency.

Though not much could be done about forests, 45 percent of the sampled institutions had attempted to correct other outside transmission problems. Options chosen to reach blind spots, included the following:

- Adding officers and a telephone at a problem location,
- Changing from a low to an ultra-high frequency (UHF) band for communicating within the facility,
- Increasing the wattage output from the main trunk station,
- Installing a repeater at a high point,
- Purchasing more powerful radios,
- Extending the base antenna,
- Buying a more powerful base station and installing a tower,
- Adding a mobile repeater,
- Raising the height of an antenna, and
- Relocating antennas.

Inside-Building Problems. Fifty-five percent of the respondents reported difficulty with two-way radio transmission from inside buildings. The most common problem (70 percent) occurred when the building design required radio transmission to pass through more than one concrete wall. Interference also arose with some regularity from other electrical equipment (40 percent) and fluorescent lights (17 percent).

Other problems that affected two-way radio transmission inside a building were feedback when two officers were talking at the same time too near each other, other facilities using the same frequencies, high-frequency interference from computers, lack of a repeater system, fading and dead batteries, old radios, and interference from the telephone system.

Only 28 percent of the respondents tried to correct these inside problems (obviously, the most common problem, building design, could not be directly solved). Solutions that had been implemented included increasing wattage output from the main trunk system, installing special antennas that ran throughout the facility, installing a repeater, installing external antennas, and increasing wattage output from transceivers.

A third (33 percent) of the respondents reported having problems caused by electronic equipment from other facilities interfering with their system (or vice versa). Where attempts had been made to correct this situation, the options pursued had been reducing power, changing radio frequencies, and buying equipment to filter out transmissions from another facility (in one instance from 65 miles away).

Other Problems

Compromise of Communications. Within the year immediately preceding the survey, reports had been rare (13 percent) concerning compromised two-way radio communications. In several of these cases, the channel was being monitored over a multiband radio; in others, an inmate took a radio from a staff member. One facility found it was broadcasting on the FM dial. Two-way radio transmissions were also reported being picked up by TV remote control and fine tuning units.

Although compromises of this type of system rarely affected institution security or operations, 33 percent of the responding facilities reported they tried to prevent it. Methods tried include the following:

- Allowing inmates access to AM/FM band radios only,
- Adding a trunk system,
- Instituting new procedures for signing out radios,
- Taking extra precautions to prevent loss of radios,
- Experimenting with radios that had digital or analog voice protection and experimenting with updating the radio console, and
- Evaluating different types of TV remote controls.

Batteries. All facilities reported using nickel-cadmium (NICAD) batteries in their radios (one also had lithium battery units). Forty-four percent of the sample facilities reported problems with radio batteries.

The NICAD batteries give a flat voltage discharge of 1.25 volts and good low-temperature operation. They are rechargeable. The NICAD battery has no special disposal requirements and it is much less expensive than lithium batteries. For responding facilities, the biggest problem with NICAD batteries by far (87 percent) was that when they were recharged too soon, their memory was shortened; unless an appropriate schedule was closely followed, the new charge did not last as long as when the battery was new. Not all (71 percent) of the facilities had a recharger package for each radio. Of the 29 percent that did not, less than a third (31 percent) thought individual rechargers would be an improvement.

Lithium batteries are made with lithium, a soft, silver-white element. The battery has a long life and operates well under extreme temperatures, particularly cold.

Responding facilities were well aware of the limitations and drawbacks of lithium batteries. They emit hydrogen gas and, therefore, must be well-ventilated when used under extreme heat conditions, since they have a tendency to explode. Lithium batteries cannot be recharged. Additionally, they are not environmentally sound and must be segregated and wrapped when being disposed. They are also much more expensive than NICAD batteries.

Maintenance and Training

Two-way radios were most often maintained under a service contract (57 percent), but sometimes by staff (34 percent), the vendor (29 percent), or the manufacturer (7 percent). Some facilities could also call on the state department of telecommunications or the state radio shop.

Where staff members did the maintenance and repair, training was provided by the manufacturer (26 percent), the facility (26 percent), or the vendor (32 percent). Some staff members were hired with the necessary expertise and others were self-taught. Just over a third (35 percent) of those responding believed a maintenance contract would reduce repair costs, and only 19 percent believed it would improve the quality of repairs.

Few facilities stocked spare parts for their radios (19 percent) or chargers (18 percent), since 85 percent found that spare parts were readily available from the manufacturer.

DURESS ALARMS

Almost all duress alarm systems (94 percent) were acquired for a particular reason. Staff safety was obviously an overriding consideration. In other cases, the systems were required by a consent decree or a union agreement. The alarms were less expensive than radios, an important factor in some jurisdictions. They also replaced radios where staff was in contact with inmates, particularly with prisons increasingly housing a larger population of aggressive prisoners.

Duress alarms were manufactured in two general types: wireless personal alarms and panic buttons.

Wireless Personal/Body Alarms

The personal alarms (a.k.a. body alarms) were duress alarms usually carried or worn by a staff member. They sometimes were part of a walkie-talkie and they sometimes had special features, such as the ability to send an alarm when the device was tilted to a predetermined angle (e.g., 30 degrees) for a specified period of time. These latter devices, found in 28 percent of the facilities, were commonly known as "staff down" or "officer down" alarms.

Usage. As Table 6-7 demonstrates, wireless duress ***alarms*** were ***least*** used by facilities that were small, fairly recently constructed, minimum security, and located in the West.

Table 6-7
Wireless Personal Duress Alarm Use

Area		Security		Opening Date		ADP	
Northeast	58%	Minimum	35%	Before 1900	100%	Under 500	17%
South	92%	Medium	81%	1900-1939	63%	500-999	74%
Midwest	67%	Maximum	73%	1940-1979	56%	1000+	100%
West	23%	Mixed	64%	1980-Present	62%		

For the 36 facilities (64 percent of the respondents) that had wireless duress alarms, body alarms were the most popular (86 percent), though a significant number of institutions (42 percent) used equipment that incorporated a walkie-talkie feature. Alarm pens were used in only one facility. Other duress alarms reported were the wireless, button-operated, personal alarm; one-way communication; and unit identification.

The average number of body alarms used in the 31 institutions replying to this question was 71, with a low of 3 and a high of 410. Fourteen facilities reported having the walkie-talkie feature (average number of units was 62-low 16 and high 138). The one facility using alarm pens had 25 of them.

In eight out of ten instances (81 percent), the amount of duress alarm equipment reported included spares for use when another unit was being serviced.

One facility's duress alarms would transmit almost 10 miles (50,000 feet); the average transmission distance was somewhat over half a mile (3,863 feet). The shortest reported transmission distance was 60 feet. Fifty-nine percent of the responding facilities reported there were no blind spots that interfered with transmission.

None of the duress alarms was location-specific. Most (81 percent) were directed by UHF transmitters, though 19 percent used very high frequency (VHF) transmitters. Almost all institutions (94 percent) processed alarm signals immediately; only 28 percent had a system to identify false alarms. Over half (58 percent) of the responding facilities logged calls automatically.

Half the sample institutions would like a type of duress alarm they did not presently own. Some wanted alarms that were location-specific, others person-specific. Very much desired was a system that would sound an alarm and permit two-way communication. The goal was to have devices that transmitted duress signals from anywhere to quickly and accurately locate personnel in trouble.

Most facilities considered their transmitters easy to use (83 percent), silent (75 percent), dependable (75 percent), light (64 percent), and inconspicuous to the point of being unnoticeable (42 percent). In general (70 percent of the cases), institutions were satisfied with their duress alarm systems. Those that were dissatisfied cited the following:

- Too many false alarms (this system was taken out of service),
- Problems because the alarms were not connected to a central receiving station,
- Unreliability of a system, perhaps because maintenance was not available,
- Limited range,
- Inability to pinpoint location of the alarm,
- Blind spots that affected transmission,
- Significant maintenance problems, and
- Stray signals from a nearby radio tower that set off the alarms.

Installation. Wireless duress alarms most often were installed by an outside contractor (53 percent), followed by the staff (30 percent), the manufacturer (13 percent), or a vendor (5 percent). In all but one case, the systems were installed to manufacturer's specifications; nevertheless 41 percent of the respondents experienced bugs after installation.

Seven institutions managed to resolve their problems within a month, the average time being 8 days. In four other facilities, problems were corrected in an average of 4 months, with a high of 6 months. At the other extreme, three institutions reported it took years to work out the bugs, for one as many as 3 years. Usually (81 percent of the cases) the systems were debugged at no additional cost to the facility.

In only two-thirds of the installations was a performance bond required of the installer, and in all these cases the installer was required to fix post-installation problems.

Maintenance and Training. Rarely (19 percent of the time) did a facility have a staff training program to maintain and repair its duress alarms. The six institutions reporting that they did provide such training indicated that the average number of hours provided was 33, with a low of 4 and a high of 100 hours.

The vendor was most likely (54 percent of the time) to provide the training, though the facility did it in 31 percent of the cases. Other institutions relied either on an outside contractor or on trial and error.

The worst-case reported of duress alarm maintenance down-time lasted 15 weeks. More typically, problems were resolved within 2 to 4 days. Not much enthusiasm for maintenance contracts was expressed by the sampled institutions: 69 percent of those responding thought they would not be cheaper, and 82 percent thought the quality of repairs would not improve. Since spare parts were readily available from the manufacturer (93 percent), only 39 percent of the facilities stocked them.

Panic Buttons

Fifty-four percent of the respondents reported having panic button devices. When a staff member pressed a wall-mounted button, an alarm was sent from that specific location, thus identifying the site of the problem. As shown in Table 6-8, they were ***least*** used by institutions that were large, old, minimum security, and located in the West or Midwest.

Table 64
Panic Button Use

Area		Security		Opening Date		ADP	
Northeast	50%	Minimum	29%	Before 1900	33%	Under 500	39%
South	67%	Medium	69%	1900-1939	50%	500-999	74%
Midwest	47%	Maximum	55%	1940-1979	50%	lOOO+	36%
West	46%	Mixed	64%	1980-Present	58%		

Conclusions and Issues

CONCLUSIONS

Institutional security and staff and inmate safety are essentials in any effective correctional facility. These, in turn, rely on the presence of efficient communication channels. Communication systems exist to transfer routine administrative information and time-sensitive matters, but are most critical in time of emergency. Reliable methods for communicating among staff and between personnel and inmates help resolve situations that are literally of a life-or-death nature.

It is important for corrections personnel to be in instant communication with each other. To make sure that this occurs and that messages/alarms can be heard clearly and easily means that a communication system should command managerial attention at the highest levels.

The equipment and support needed will depend on the location of the facility, its configuration, population of the institution, and staff support requirements.

When properly planned and maintained, communication systems will be responsive to an institution's changing missions and demographics and to improvement in technology. In addition to being able to effectively respond to problems, a good communication system can prevent them.

Telephone Systems

The most universally present technological system in corrections, as reflected in the survey's 56 replies, was the telephone. It was used in three ways:

An inmate telephone system, used by prisoners to communicate with outside society, generally did not allow incoming calls (93 percent) but permitted outgoing collect calls (89 percent). Some of the systems restricted calls to certain numbers (61 percent) and recorded such data as date, time, and number called (45 percent).

Twenty of the responding facilities had fraud prevention capabilities built into their phone systems. Of these, 9 limited the amount of time permitted per call, 12 blocked calls to unauthorized numbers, and 13 recorded or monitored calls.

The number of inmates per phone ranged from 5:1 to 277:1; the most frequent ratio (reported by 16 respondents) was between 21:1 and 30:1.

Visiting room phones were available for use by visitors in the facility's visiting room. Efforts to keep this system tamper-proof were generally successful (78 percent of the replies). Like other phone systems, visiting room telephones were rarely down for repairs.

Staff telephone systems were used for intrastaff communications. Half (51 percent) of the reporting institutions had their phone system programmed with a group-call option that allowed certain numbers to be called to summon staff help during an emergency. Forty-eight percent of these systems had a feature that sounded an alarm if the phone was off the hook too long.

More than half (58 percent) of the respondents mentioned features they would like to see added to their present system. Among the most frequently cited were interface with pocket-pagers, group calling, automatic call-back, a dedicated emergency phone, off-the-hook alarm capability, and an override ability to cut into calls made from selected phones. All desired features related to security rather than convenience.

Overall, there appeared to be general agreement that these systems provided adequate equipment that was reliable and relatively quick to repair.

Intercom Systems

Thirty-eight percent of the sampled institutions reported some environmental problem with their intercom systems. Of these, the one most often mentioned was difficulty in transmitting over long distances.

Tampering by inmates, however, was cited more frequently than the environment as being a problem. The solution seemed clear: Facilities that reported having tamper-resistant intercom systems also mentioned that substations were not accessible to inmates. The downside of this solution for tampering was that locating substations where inmates could not get to them also meant that they were not available for use as duress alarms.

Two-Way Radios

Two-way radios were almost as universal in corrections as telephones-only three facilities did not report using them; all but one institution (a minimum security facility) considered them critical to security.

The survey indicated that one major problem with two-way radios concerned the use of nickel-cadmium (NICAD) rechargeable batteries. If the batteries were recharged before they were totally depleted, their subsequent available charge was reduced to the amount that had been used previously, in what was termed the “memory effect.” For example, if an 8-hour battery was recharged after only 6 hours of use, its subsequent time-to-recharge became 6 rather than 8 hours.

Transmission problems, a second area of difficulty for two-way radios, were more likely to occur outside (80 percent) than inside (55 percent) facilities. In both instances, the worst obstruction was a wall. Outside, 48 percent of transmission blockages were caused by other buildings; inside, 70 percent were caused by attempts to transmit through more than one concrete wall.

Solutions proposed to remedy this situation were almost invariably technological: installing repeaters, buying more powerful radios, and raising or moving antennas. Only one facility suggested adding officers and telephones.

Duress Alarms

Duress alarms allowed corrections personnel to send a signal to a 24-hour staffed control center when an emergency occurred. Blind spots were cited as a problem for 14 (25 percent) of the facilities that responded to this question. Of these, 93 percent used body alarms to transmit up to 2,500 feet; for longer distances, walkie-talkies were&o provided.

The biggest negative reported for personal/body duress alarms was that they reported only that there was a problem, but did not indicate where the problem was. Alarms that would signal where in the facility the emergency was occurring were high on institutions’ wishlists. Location-specific alarms would allow a quicker response. Perhaps Med-Alert alarm technology that ties into the phone system could be adapted for use in corrections; it would trip the nearest telephone extension and flash a light on a control panel.

Wall-mounted panic button duress alarms were used by some facilities (54 percent) to address the problem of site identification. When the button was pressed, an alarm was sent that identified the specific location of the problem (since the panic button's location coincided with the location of the problem).

ISSUES

Corrections administrators, planners, and fiscal officers were faced with a myriad of choices when acquiring or upgrading communication systems for new or existing institutions. Prudent managers should review available comparative information and consult with communications experts prior to making these decisions.

When communication systems are being installed and/or upgraded the following issues should be thought through:

1. Prepare a list, with input from staff, of the requirements the new system should meet.

2. Consider all possible solutions to meet the communication system requirements in order to make the most cost-efficient decisions.

3. Check plans with colleagues in other institutions and systems to benefit from their experiences.

4. Ensure that equipment is purchased for which parts will be readily available, and will remain available, once the system is installed.

5. Consider available optional telephone features, such as interface with pocket pagers, group calling capabilities, automatic call-back, dedicated emergency phones, off-the-hook alarms, call override, cellular phones, recording capabilities, monitoring features, and hearing-aid compatibility. Also consider the following:
   - Whether the intercom network should be part of the telephone system or separate,
   - Whether or not to use the telephone system for paging,
   - Whether certain numbers should be blocked so that inmates cannot reach them, and
   - Where in the facility the telephones should be installed.

6. Check with phone companies in regard to profit-sharing plans that may be available.

7. Determine the number of inmate telephones needed in relation to size of population.

8. Develop telephone procedures to reduce the likelihood of fraudulent use by inmates.

9. Take into consideration environmental factors that may affect a radio system's effectiveness, such as the following:
   - Configuration of the buildings,
   - The amount of metal in the buildings,
   - Other obstacles that might affect clear transmissions (trees, hills, etc.),
   - Nearby institutions that might be using the same radio frequencies,

- Long transmission distances that may require powerful radios, and
- Potential blind spots that may require extra wiring or antennas for clear transmission.

10. Consider battery life and recharging capabilities for walkie-talkie radios.

11. When determining number of walkie-talkies to be purchased, consider the need for back-ups when radios are being recharged and/or repaired.

12. Develop accountability procedures for signing out radios.

13. Consider audio monitoring as part of the housing units' intercom system.

14. Ensure speakers are installed to be easily heard but out of reach for inmate tampering.

15. Check plans for communication system installations using realistic, simulated situations, prior to activation.

16. Ensure that the various systems being installed can be integrated with each other. Test system components.

17. Ensure that the vendor provides detailed drawings of the system after it is in place to simplify maintenance and repair.

18. Have a trained staff member monitor installation to ensure that the installers are properly trained and working effectively.

19. Make decisions as to who on staff should be trained to operate each system and what training schedule will be followed.

20. Ensure that the manufacturer provides a preventive maintenance schedule at the time of installation.

21. Have the manufacturer provide a maintenance contract (preferable to an independent contractor).

22. Select equipment for which local contractors can provide 24-hour service for each system.

23. Ensure that warranties are explicit as to what is covered. Make sure the system's warranties cover not just communications equipment but transmission lines and wiring also.

24. Ensure that warranties will not run out before the installation is completely debugged.

25. Ensure that the contractors have a performance bond, and then require the bonded contractor to fix any post-installation problems.

Under no circumstances should corners be cut on funding for electronic communication systems, as they are the facility's life-line for maintaining security and protecting staff and inmates.

Chapter 6

Questionnaire Data-Communication Systems

Intercom Systems	51	Wireless Duress Alarms	36
Master/Base Stations	56	Two-Way Radios:	
Panic Buttons	30	Vehicle Radios	53
Telephones	56	Walkie-Talkies	53
Other (specify)	9		

Intra-Facility Communication Systems
51 Responses

1. How many master stations does the facility's intercom system have?
# of Responses - 47 Average # of Master Stations - 4.34 High 30 Low 1

2. How many substations does the facility's intercom system support?
# of Responses - 40 Average # of Substations - 38.98 High 484 Low 1

3. Where are the substations located? [Check (x) ALL that apply]

Housing Units	35
Sally-Ports	20
Outside of Entrances	24
Hallways	19
Offices	28
Other (specify)	20

4. Are substations accessible to inmates?
Yes 17 No 27 Don't Know 4 No Response 7

5. Do you believe there should be more substations?
Yes 12 No 31 Don't Know 1 No Response 7

6. If yes, where should they be located? (covered in text)

7. Were substations sufficiently tamper-resistant as installed?
Yes 27 No 14 Don't Know 4 No Response 6

8. Is connection between the substations and master stations immediate?
Yes 37 No 4 Don't Know 4 No Response 6

9. If no, how long does it take for the substations to be connected to the master stations?
# of Responses - 0

		Yes	No	Don't Know	No Response
10.	Does the system offer the flexibility for all stations or selected stations to communicate on a conference basis?	18	26	3	4
11.	Does the intercom system allow staff to monitor sounds from areas under their jurisdiction? (e.g., housing units)	33	15	0	**3**
12.	Does the intercom system serve as an inmate duress alarm?	14	35	0	**2**
13.	Do any environmental factors (i.e. distance) affect transmission?	5	40	3	**3**

14. If yes, to what degree is transmission affected by each of the following factors? [For "a" through "d" place an (x) in the appropriate column.]

	Affected	Somewhat Affected	Not Affected	Don't Know	No Response
a. Steel	1	1	5	1	44
b. Concrete	1	1	5	1	43
c. Distance	3	1	4	1	42
d. Other (specify)	3	0	3	1	44

		Yes	No	Don't Know	No Response
15.	Can the system be operated hands-free?	12	37	0	2
16.	Are the master stations automatically alerted if there is a problem within the system (short, cut wire, etc.)?	6	40	2	3
17.	If yes, does the system have a graphic display to indicate the location of the problem?	3	28	0	20
18.	Does a problem in one area of the intercom system block the operation of the entire system?	4	42	3	2
19.	Does the intercom system interface with other electronic equipment?	12	30	2	7

20. If yes, what other electronic equipment does it interface with? [Check (x) ALL that apply.]

Phone System	8
Two-Way Radios	1
Public Address System	6
Access Control System	3
Other(specify)	1

		Yes	No	Don't Know	No Response
21.	Can paging be accomplished on a zone-by-zone basis?	34	15	1	1
22.	Does the facility have a regularly scheduled maintenance/testing program for the intercom system?	23	27	0	1

23. If yes, how often is maintenance/testing performed and what does it involve? (covered in text)

Weekly	0
Monthly	0
Quarterly	4
Semiannually	3
Annually	0
Randomly	4
Other (specify)	5

24. Who performs the scheduled maintenance/testing and what are they responsible for? (covered in text)

Staff	21
Vendor	4
Outside Contractor	4
Other (specify)	2

25. If the facility has scheduled maintenance/testing, are there many problems that require repairs?
Yes 8 No 21 Don't Know 3 No Response 19

26. What are the three most common repairs? (covered in text)

Wireless Duress Alarms
(36 Responses)

1. What type of wireless duress alarms are used in this facility? [Check (x) ALL that apply.]

Alarm Pens	1
Body Alarm	31
Walkie-Talkie Feature	15
None	16
Other (specify)	5

How many of each unit does the facility have?

Alarm Pens
# of Responses - 1
Average # of Units - 25
High Low

Body Alarms
# of Responses - 30
Average # of Units - 70.7
High 410 Low 3

Walkie-Talkie Feature
# of Responses - 14
Average # of Units - 61.64
High 138 Low 16

Other (refer to Question #l)
# of Responses - 2
Average # of Units - 72.5
High 85 Low 60

3. Does this number reflect spare units that can be used when others are being serviced?
Yes 29 No 7 Don't Know 0

4. Can the alarm be set off automatically as well as manually? (e.g., If the alarm is tilted at a specified angle for a given period of time, it will be set off.)
Yes 10 No 26 Don't Know 0

5. The transmitter is [Check (x) ALL that apply]:

Silent	27
Discreet	15
Easy To Use	30
Light	23
Dependable	27

6. How far will the transmission go in open areas?
# of Responses - 28 Average - 3,863.39 Feet High 50,000 Feet Low 60 Feet

7. Are there blind spots in the facility from which the duress alarm will not function effectively?
Yes 14 No 20 Don't Know 2

8. The duress alarms are [Check (x) ONE]:

Ultrasonic location-specific	0
UHF transmitter-specific	25
Don't Know	7

		Yes	No	Don't Know
9.	Is there a system to eliminate or identify false alarms?	10	26	0
10.	Is the alarm signal processed immediately?	34	2	0
11.	Is there a system that logs calls?	21	15	0
12.	Is there a type of duress alarm that this facility does not have that you would like to have?	15	15	6

13. If yes, what type of duress alarm is it? (covered in text)

14. Why would this type of duress alarm be better than what the facility already has? (covered in text)

15. Were the wireless duress alarms acquired for a particular reason or to solve a specific problem?
Yes 32 No 2 Don't Know 2

16. If the duress alarms were acquired for a specific reason, what was that reason? (covered in text)

17. Have the duress alarms met expectations in terms of solving the problem?
Yes 23 No 10 Don't Know 0

18. If they have not solved the problem, why? (covered in text)

Telephone Systems
(56 Responses)

Inmate Phone Systems (Phone service for inmates' use in making personal calls)

1. Does this facility have phones for inmate use only?
Yes 55 No 1 Don't Know 0

2. If yes, how many phones are there for inmate use?
# of Responses - 54 Average # of Phones - 32.94 High 120 Low 2

3. Does the number of phones adequately handle the needs of the inmate population?
Yes 49 No 4 Don't Know 1 No Response 2

4. If no, how many more phones do you believe are needed?
# of Responses - 7 Average # of Phones - 20.71 High 112 Low 1

		Yes	No	Don't Know	No Response
5.	Does the inmate phone system limit time per call?	21	33	1	1
6.	Does the inmate phone system offer call block for numbers that are restricted?	28	26	1	1
7.	Does the phone system offer anything other than collect calling?	6	48	1	1
8.	Does the inmate phone system record data such as date, time, called numbers?	23	28	4	1
9.	Are incoming calls possible on the inmate phone system?	4	50	0	2
10.	Does this facility monitor inmate phone calls?	24	30	0	2

		Yes	No	Don't Know	No Response
11.	Does this facility record inmate phone calls?	22	31	1	2

		Monitored	Recorded
12.	If yes, the calls are monitored/recorded [Check (x) ONE]:		
	Randomly	12	2
	On a Selected Basis	12	5
	Continuously	6	10
	Don't Know	1	1
13.	If the phone calls are monitored/recorded on a selected basis, they are selected by [Check (x) ALL that apply]:		
	Institution	**9**	**8**
	Housing Unit	**6**	**4**
	Individual Inmate	**7**	**2**
	Other (specify)	**2**	**0**

		Yes	No	Don't Know	No Response
14.	Is the system hearing-aid compatible?	13	24	18	1
15.	Do the inmate phones have handsets?	49	3	3	1
16.	Was the inmate phone system sufficiently tamper-resistant as installed?	42	10	3	1
17.	Does the phone system offer a system for fraud prevention?	20	22	13	1

18. The inmate phones were:

Purchased	8
Leased	5
Supplied by a Vendor	42
Other (specify)	0

Visiting Room Phones (Phones used for non-contact visiting)

1. How many phones does the facility have for non-contact visiting?
# of Responses - 18 Average # of Phones - 10.11 High 55 Low 2

2. Does the number of phones adequately address the needs of the facility for visits?
Yes 16 No 2 Don't Know 0 No Response 38

3. If no, how many more phones are needed?
# of Responses - 2 Average # of Phones Needed - 10 High 16 Low 4

		Yes	No	Don't Know	No Response
4.	Are the phones sufficiently tamper-resistant as installed?	14	4	0	38
5.	Does the visiting room phone system offer a system for monitoring visits?	7	10	1	38
6.	Is this phone system hearing aid compatible?	6	11	1	38

Institution/Staff Phone Systems

		Yes	No	Don't Know	No Response
1.	Is the institution/staff phone system interfaced with the intercom system?	10	46	0	0
2.	Is the institution/staff phone system used for site-wide intercom?	14	41	1	0
3.	Does the institution/staff phone system interface with pocket pagers?	14	41	1	0
4.	Does the institution/staff phone system interface with the PA system?	11	44	1	0
5.	Is the institution/staff phone system a PBX system?	35	13	8	0
6.	If yes, is the PBX memory-supported?	29	9	11	7
7.	Does the system include a group call system to permit calling a predetermined set or sets of phone numbers in the event of an emergency as a means of summoning staff?	27	26	2	1
8.	Does the institution/staff phone system feature an off-hook alarm for staff?	26	28	2	0
9.	Is there a system for logging calls?	35	20	1	0

		Yes	No	Don't Know	No Response
10.	Does the institution/staff phone system feature line monitoring to detect and report faults in lines? (i.e., shorts)	18	27	11	0
11.	Does a fault in one line block the operation of the entire system?	3	45	7	1

12. Does the phone system offer an [Check (x) ONE]:

Emergency Alert Number	8
Off-the-Hook Alarm	11
Both	15
Don't Know	13

13. The phone system is [Check (x) ONE]:

Leased	10
Purchased	41
Don't Know	4

14. Are there features that are not currently part of the institution/staff phone system that you believe would be beneficial?
Yes 25 No 18 Don't Know 11

15. If yes, please list these features in order of importance with #l being the most important (covered in text)

16. How would these features make the institution/staff phone system more effective? (covered in text)

Two-Way Radios
(56 Responses)

		Yes	No	Don't Know
1.	Does this facility use two-way radios?	55	1	0
2.	If yes, is the use of two-way radios an important security feature for staff safety?	54	2	0

3. If yes, what would the effect on the security of the facility be if the two-way radios were removed? (covered in text)

4. How many hand-held radios does the facility have?
# of Responses - 54 Average # of Hand-held Radios - 66.48 High 255 Low 4

		Yes	No	Don't Know	No Response
5.	Does this number include radios that are used for back-up while others are being repaired or recharged?	47	7	0	2
6.	Are the hand-held radios used to maintain contact between officers inside the facility and officers outside of the facility?	53	2	0	1

7. What is the longest range that the radios are needed to transmit outside of the facility?
# of Responses - 32 Average - 2676.94 Feet High 7000 Low 15

8. Have there been problems with obstructions that limit the range of transmission?
Yes 45 No 11 Don't Know 0

9. If yes, what types of obstructions have been encountered? [Check (x) ALL that apply.]

Other Buildings	27
Hills	27
Other (specify)	16

10. Has anything been done to correct this problem?
Yes 20 No 24 Don't Know 0 No Response 12

11. If yes, briefly explain (i.e., the use of a station to amplify the signal from the radio and retransmit from a high antenna). (covered in text)

12. What is the longest range that radios are needed to transmit within the facility?

# of Responses - 49	Average - 1979.39 Feet	High 6000	Low 1000
# of Responses - 6	Average - 5.67 Miles	High 25	Low 1

13. Have staff encountered problems with the quality of transmission within the facility?
Yes 30 No 25 Don't Know 0 No Response 1

14. If yes, what is the cause of the problem? [Check (x) ALL that apply]

The configuration of the building requires transmission to pass through more than one concrete wall.	21
Other Electrical Equipment	12
Fluorescent Lights	5
Other (specify)	11

15. Has anything been done to correct this situation?
Yes 8 No 21 Don't Know 0 No Response 27

16. If yes, please describe (e.g., run special antennas along ceiling to carry the signal). (covered in text)

	Yes	No	Don't Know	No Response
17. Has this facility experienced problems with equipment being activated by electronic equipment from other facilities or vice versa?	18	36	1	1
18. If yea, has anything been done to correct this situation?	4	14	0	0

19. If yes, please describe (e.g. installing a trunked communication system). (covered in text)

20. Have communications on the hand-held radios been compromised at any time during the last year?
Yes 7 No 45 Don't Know 3 No Response 1

21. If yes, what were the circumstances? [Check (x) **ALL** that apply.]

Inmate(s) confiscated a radio from a staff member.	1
Inmate(s) had a VHF scanner.	0
Bugging devices were being used to monitor channels in use.	0
Channel was being monitored over a multi-band radio.	3
Other(specify)	6

	Yes	No	Don't Know
22. Did the compromise of the communication system affect the security and/or the operation of the facility?	5	7	0
23. Has anything been done to prevent this from occurring in the future?	4	8	1

24. If yes, briefly explain (e.g., installed a trunked/encrypted/secured communication system). (covered in text)

25. What type of batteries does this facility's hand-held radios have? [Check (x) ALL that apply.]

Nickel-Cadmium (NICAD)	56
Lithium	1

26. Have there been problems associated with your use of either type of battery?
Yes 23 No 29 Don't Know 3 No Response 1

27. If yes, please explain the circumstances (e.g., with the NICAD, the memory effect requires that the battery be totally depleted before it is recharged). (covered in text)

28. Does the facility have a recharger package for each radio?
Yes 40 No 16 Don't Know 0

29. If no, do you believe that having a recharger package for each radio would be an improvement?
Yes 5 No 11 Don't Know 0

30. Who is responsible for the maintenance/repair of the hand-held radios? [Check (x) ALL that apply.]

Staff	19
Vendor	16
Manufacturer	4
Service Contract	32
Other(specify)	9

31. If staff, who provides the training for maintenance/repair of the radios?

Facility	5
Vendor	4
Manufacturer	5
Other (specify)	6

32. If staff is responsible for the maintenance/repair of the radios, do you believe a service contract would be an improvement?

a. For Cost	Yes 6	No 11	Don't Know 1	No Response 38
b. For Quality of Repairs	Yes 3	No 13	Don't Know 1	No Response 39

33. What percentage of staff members is trained to maintain/repair the hand-held radios?
# of Responses - 18 Average - 8.70% High 100% Low 1%

	Yes	No	Don't Know	No Response
34. Does the facility stock spare parts for key components of the:				
a. Radios	10	42	1	4
b. Chargers	9	42	0	5
35. Are spare parts readily available from the manufacturer for:				
a. Radios	40	7	6	3
b. Chargers	41	7	5	3

36. Were hand-held radios acquired for a particular reason or to solve a specific problem?
Yes 40 No 11 Don't Know 2 No Response 3

37. If the radios were acquired for a specific reason, what was that reason? (covered in text)

38. Have the radios met expectations in terms of solving the problem?
Yes 46 No 1 Don't Know 1 No Response 8

39. If they have not solved the problem, why? (covered in text)

General Information

The following group of questions addresses general information that is applicable to each of the communication systems covered in this questionnaire. As you complete this section please answer every question with the appropriate response in each of columns "A" through "E" as they correspond to the systems indicated below.

A = Intra-Facility Communication System
B = Wireless Duress Alarms
C = Inmate Phones
D = Visiting Room Phones
E = Institution/Staff Phones

	A	B	C	D	E
1. Who installed the system? [Check (x) ONE]					
Manufacturer	8	5	10	2	13
Outside contractor	35	21	42	13	37
Staff	8	12	2	8	7
0ther(specify)	2	2	1	0	1
2. Was the system installed according to the manufacturer's specifications?					
Yes	43	33	48	19	49
No	2	1	1	0	1
Don't Know	6	3	6	4	6
No Response	5	19	1	33	0
3. Did the facility experience bugs in the system after installation was complete?					
Yes	23	15	21	5	21
No	21	22	27	16	29
Don't Know	2	1	6	2	5
No Response	7	18	2	33	1
4. If yes, for how long? (covered in text)					
5. Was the system successfully debugged?					
Yes	20	15	20	7	22
No	6	4	2	1	3
Don't Know	2	0	3	0	2
6. Were additional funds required to debug the system?					
Yes	6	3	3	1	4
No	15	13	15	5	14
Don't Know	6	4	7	2	8

A = Intra-Facility Communication System
B = Wireless Duress Alarms
C = Inmate Phones
D = Visiting Room Phones
E = Institution/Staff Phones

	A	B	C	D	E
7. The specifications were written by [Check (x) ALL that apply]:					
Facility	19	17	22	11	**24**
Consultant	22	13	16	12	19
Vendor	14	10	21	5	18
There are no specifications	4	2	2	1	1
Other (specify)	6	7	7	1	8
8. Was a performance bond required of the supplier/ vendor/installer?					
Yes	17	15	16	8	18
No	11	8	10	7	10
Don't Know	22	16	28	9	27
No Response	6	17	2	32	1
9. Was the supplier/vendor/ installer held to the performance bond?					
Yes	14	13	13	6	14
No	8	7	8	7	9
Don't Know	23	17	29	10	28
No Response	11	19	6	33	5
10. Who is responsible for the maintenance/repair of the system? [Check (x) ONE.]					
Staff	34	15	9	18	**24**
Manufacturer	5	4	9	2	7
Outside Contractor	16	17	38	37	28
Other (specify)	2	2	5	2	4
11. If staff, does the facility have an established training program in which staff learn to maintain/repair the system?					
Yes	8	5	4	6	9
No	31	21	21	15	25
12. How many hours of training are required for staff to learn to maintain/repair the systems? (covered in text)					
13. Which staff are trained to maintain/repair the systems? [Check (x) ALL that apply.]					
Line Officers	3	3	1	1	1
Technicians	27	15	13	14	23
Other (specify)	4	4	3	3	3

A = Intra-Facility Communication System
B = Wireless Duress Alarms
C = Inmate Phones

D = Visiting Room Phones
E = Institution/Staff Phones

	A	**B**	**C**	**D**	**E**
14. The training is provided by [Check (x) ALL that apply]:					
Vendor	11	7	8	6	15
Facility	7	4	2	5	7
Other(specify)	6	2	2	2	1
15. What is the average amount of down-time per year for maintenance/repairs of the systems? (covered in text)					
16. If staff now perform maintenance/repairs, do you believe a maintenance contract would be an improvement?					
a. For Cost					
Yes	6	5	2	1	5
No	23	11	11	17	20
Don't Know	3	3	1	3	0
b. For Quality of Repairs					
Yes	6	3	1	0	3
No	24	14	12	18	22
Don't Know	2	3	1	3	0
17. Does the facility stock spare parts for key components of the system?					
Yes	23	12	12	15	25
No	21	19	22	8	20
Don't Know	3	0	2	0	3
18. Are spare parts readily available from the manufacturer?					
Yes	33	25	28	20	37
No	4	2	0	0	4
Don't Know	8	23	9	3	7

Chapter 7

Management Information Systems in Correctional Facilities

Abstract

Correctional Technology: A User's Guide is the product of a nationwide assessment of the experience correctional administrators have had with various types of technological systems. The purpose of this guide is to provide correctional administrators with a user-friendly source of information to aid planning and decisionmaking.

For this chapter on management information systems (MIS), survey questionnaires were prepared, reviewed by experts in the field of MIS in corrections, pilot-tested onsite, and revised in light of that input. The final version was sent to 49 correctional institutions selected to represent all areas of the country and all levels of security. Presurvey letters and follow-up telephone calls resulted in a 96 percent response rate.

The two basic types of MIS equipment are hardware and software. Over 75 percent of the sampled institutions used standardized technologies which increased efficiency. Three general categories of software were used: inmate-related applications, administrative/facilities support programs, and identification systems.

Corrections officials were unanimous in describing MIS as essential to their work. However, their biggest complaint was that their systems were underutilized. The survey data suggest that this situation resulted from poorly designed MIS systems and a lack of sufficient equipment and adequate training.

Table of Contents

LIST OF TABLES

Executive Summary

Forty-nine institutions were invited to reply to the Management Information Systems (MIS) questionnaire; 96 percent responded. These facilities were randomly distributed in terms of their security level and location across the country. The majority of them (68 percent) were built since 1940. In regard to average daily population (ADP), there was no statistically significant relationship. The ADP of the sampled institutions was randomly distributed.

There are two types of MIS equipment: hardware and software. The former consists of things you can actually touch, such as computers, keyboards, display screens, disks, and disk drives. Software provides the instructions that operate the hardware.

A large number of facilities had standardized their hardware (74 percent) and software (80 percent). This was also characteristic of entire departments of corrections: 70 percent had standardized their hardware and 76 percent their software. Where such standardization had not occurred, efficiency was reduced (e.g., general information had to be entered separately for each program application).

HARDWARE

The number of different types of hardware per sample institution ranged from 1 to 6 (the average was 2.9; the mode, found in 18 facilities, was 3). Over half of the sample institutions used wide area networks (61 percent), mainframes (54 percent), and/or mini-computers (52 percent).

Fifty-six percent of the sample institutions reported no bugs when their hardware systems were installed. Those that experienced problems were able to correct them in a maximum of 3 months (average debugging time was 3 to 6 weeks).

SOFTWARE

The average number of software programs per facility was 23.4 (ranging from a high of 40 to a low of 11). These comprised three general categories:

- Inmate-related applications (96 percent of the respondents);
- Administrative/facilities support programs (85 percent of the sample); and
- Identification systems (24 percent of the responding facilities).

The most frequently used type of programs for inmate-related areas concerned admissions/releases (96 percent), parole (87 percent), prior criminal record (80 percent), and good time (80 percent). In the administrative category, programs were used most often for payroll (85 percent), accounts payable (78 percent), and personnel leave status (76 percent).

Software problems, encountered by 67 percent of the respondents, tended to take somewhat longer than hardware glitches to resolve, 6 to 8 weeks on average. Additionally, when compared with their experience with MIS hardware, twice as many (18 percent) institutions reported paying more than planned for debugging their software.

While there was general agreement about the usefulness of MIS, respondents still had an extensive wish list of applications for which they would like to have programs (e.g., tracking discipline, grievances, package deliveries, visitation records, personal property, food service inventory, a menu and recipe system, budget line items, transportation schedules, medical records, and a fingerprint library).

Despite the clear indication (100 percent of the replies) that MIS was critical to the effective operation of their institution, the sampled facilities believed their MIS systems were underutilized.

TRAINING

Among the respondents who reported underused MIS, 70 percent did not require their staff to be computer-literate. On average, 23 percent of a facility's personnel received 7 hours of training on hardware and 15 hours on software. Not only was the amount of training an issue, its quality also appeared to be problematical. Often (87 percent of replies) where underutilization was reported, training was provided by in-house staff "who had an interest in MIS." Moreover, once the initial session was completed, over 60 percent of the facilities provided no refresher training.

OTHER FACTORS

Several additional factors contributing to MIS underutilization were cited by the respondents:

- MIS inflexibility that made it less able to meet current demands,
- Hardware shortages that limited MIS's ability to service all staff who needed to use the system, and
- Lack of onsite support to whom staff could turn with problems.

MAINTENANCE

Preventive maintenance was a priority for about one out of four of the sampled institutions. Unscheduled repairs (reported by 63 percent of the respondents) had kept information systems down for as long as 6 weeks. In 61 percent of the facilities, in-house staff had the responsibility for keeping MIS up and running.

Ninety-eight percent of the respondents did ***not*** permit inmates to be involved in the repair or maintenance of the MIS hardware. Almost all of the reporting facilities (91 percent) had written policies to protect the security of both the hardware and software in their information systems. Other topics covered by policy statements were back-up procedures, software documentation, staffs personal use of computers, storage, and archive procedures.

SATISFACTION

Corrections officials were unanimous in describing MIS as essential to their work, yet more than half reported their systems being underutilized. Despite a number of concerns, 58 percent of the administrators indicated that they were satisfied with their management information systems. MIS technology was created to serve staff needs. Therefore, in the planning and design of these systems, staff expected to use the technology should be included throughout the process.

Introduction

Today managing information is at least as important as managing people-in fact, information is needed to better manage people. Corrections administrators surveyed were unanimous in describing management information systems (MIS) as essential to their work. Yet 51 percent thought that their systems were underutilized. This paradox was caused when staff who were not technically trained, found themselves confronted with an unfamiliar and, therefore, intimidating technology.

Managers need accurate and timely data to support a wide variety of administrative decisions. The sheer quantity of data accumulating today cannot be used effectively without technological assistance. Managers have to think short-range about manpower allocation, purchasing, inventories, tracking inmate accounts, bed space, and the state of their current budget. They must think long-range about what caseloads and institution populations will be like, what construction and renovation will be needed, and how much it will all cost in future (as well as current) dollars. If there were no machines to process the numbers, administrators would need more staff; reports processed by hand would contain more errors; institutional data and inmate histories would be harder to obtain and keep current; managers would have more difficulty communicating with other institutions; and agencies could become so inefficient as to be virtually inoperative.

Consequently, MIS technologies are needed in correctional facilities. For these technologies to function efficiently, staff resistance to change must be overcome, and the difficulties involved in integrating old and new systems must be anticipated and conquered.

The intent of this chapter is to help corrections administrators think about what needs to be done, if anything, to make their own information system more effective, and assess where their MIS technology stands in comparison with that in other correctional jurisdictions.

The objective of this chapter is to provide corrections administrators with information relevant to decisionmaking about management information systems technology. It includes the following:

- A description, in nontechnical terms, of the types of technology in use;
- An indication of support systems and staff needed to install, operate, and service the various systems;
- Factors to be considered during the selection and planning for the use of technology; and
- Conditions under which particular technologies may be appropriate, reliable, effective, or efficient.

This chapter contains the following:

- An overview of management information systems,
- A description of the characteristics of the institutions sampled in the survey,
- An analysis of the survey findings,
- Conclusions drawn from survey results, and
- Issues to consider when evaluating a management information system.

Management Information Systems: An Overview

Management information systems consist of hardware (i.e., things you can actually touch, like disks, disk drives, display screens, or keyboards) and software (i.e., the instructions that tell the hardware how to do the desired task).

MIS HARDWARE

Mainframe computers are big and expensive. Hundreds of people can work with them simultaneously, using different programs to do different things. (The only computer larger than a mainframe is a supercomputer-used exclusively in highly sophisticated scientific research-which is usually programmed to do just one thing incredibly fast.)

Mini-computers usually support from 10 to 200 users. The most powerful of these are difficult to distinguish from mainframes.

Micro-computers are more generally known today as personal computers (PCs), because they are designed for a single user. The core element in their design is a micro-processor-the central processing unit (CPU)-which is a single chip that holds all the operating information the computer needs. PCs are generally used in business for word processing, accounting, desktop publishing, and analyzing data on spreadsheets or extracted from files stored in the computer's memory.

Workstations are more powerful PCs used for engineering, desktop publishing, software design, and applications that need high-quality graphics in addition to normal computing power. Workstations are often linked together as:

- **Local area networks** (LANs) that operate within a single building or a relatively small complex of buildings. LANs allow users, while seated at their own computers, to work not only with their own CPUs, but also to interact with data from other computers in the network. LAN users can also "write" to each other electronically (E-mail). LANs can be linked to other LANs.
- **Wide area networks** (WANs) that connect computers across the country or around the world through telephone lines or radio signals.

MIS SOFTWARE

Software is anything that can be stored electronically or that directs the operation of MIS hardware. There are two general kinds: systems software and applications software.

Systems software is a set of instructions that makes the computer itself function. The best known is the disk operating system (DOS). It may be thought of as the mind of the computer.

Applications software is a set of instructions that the computer uses to do what you want it to do. It turns an idea into something that can actually be touched. Some software can be used in any kind of business or institution:

- Accounting applications to track financial matters (e.g., accounts receivable or payable, inmate accounts, or payroll);
- Inventory control programs to monitor what comes into the facility (e.g., equipment, supplies, food) and where it goes, adding items as shipments come in and subtracting them when used, thereby, keeping a running total of on-hand items;
- Operations applications to track what is done to keep the facility running smoothly (e.g., maintenance, repairs, laundry, medical, and food service); and
- Personnel applications to record hires, terminations, scheduling, leave, training, and performance ratings.

Other types of software have been designed specifically for correctional use:

- Inmate applications to record and monitor what happens to inmates (e.g., property control, visits, victim restitution records, and training and work assignments);
- Case management applications to track admissions records, and to review parole decisions, release dates, and records (including prior arrests and convictions); and
- Identification (ID) systems to maintain population statistics and monitor the movements of staff and inmates. Some programs integrate other types of data (e.g., commissary, meals, library loans) into the ID systems. (Because only 11 facilities-24 percent of respondents-reported having automated ID systems, generalizations about the systems cannot be made in this user’s guide.)

Law enforcement databases are usually accessible by network rather than kept facility by facility. The best known of these networks is probably the information available from the federal National Crime Information Center (NCIC). Facilities use such databases to supplement their case management information (e.g., checking an inmate’s outstanding warrants/detainers) and frequently will have an NCIC-dedicated computer.

Sample Characteristics

The MIS questionnaire elicited 46 responses (a 96 percent response rate). Using the regional boundaries defined by the Bureau of Justice Statistics, the facilities responding were well distributed throughout the country: 20 percent in the Northwest, 26 percent in the South, 35 percent in the Midwest, and 19 percent in the West. They represented all security levels: 22 percent minimum, 30 percent medium, 13 percent maximum (long-term difficult inmates), and 35 percent mixed (no single inmate group making up more than two-thirds of the population).

There was a good mix of population size as well; 40 percent had fewer than 500 inmates, 30 percent had 500 to 999, and the remaining 30 percent had 1,000 or more. The larger facilities were mainly in the Midwest. More than a third (35 percent) of the sample facilities were relatively new-built since 1980.

LOCATION AND SECURITY LEVELS

Table 7-1 shows the distribution of the 46 respondents. Most responding institutions were located in the Midwest (35 percent), followed by the South (26 percent), and the Northeast and West (20 percent and 19 percent respectively). Table 7-2 shows the levels of security of the respondents.

Statistical analysis of the data used to develop Tables 7-1 and 7-2 reveals a nonsignificant (N.S.) relationship between the number of respondents in each security category and geographic area.* In other words, the distribution of security levels across the geographic locations was random.

Table 7-1
Location of Sample Facilities

Location	n	%
Northeast	9	20
South	12	26
Midwest	16	35
West	9	19
Total	46	100

AGE OF SAMPLE FACILITIES

All 46 respondents provided data concerning the date when their institutions had been constructed. Most of the sampled facilities were opened since 1980 (35 percent). Table 7-3 displays date-of-construction data for all respondents.

* $\chi^2 = 3.661$; df=6; N.S.

Table 7-2
Security Level of Sample Facilities

security Level	n	%
Minimum	10	22
Medium	14	30
Maximum	6	13
Mixed*	16	35
Total	46	100

* Inmate population was less than two-thirds in any security category.

Table 7-3
Date Facilities Opened

	n	%
Before 1900	5	10
1900-1939	10	22
1940-1979	15	33
1960-Present	16	35
Total	46	100

POPULATION SIZE OF SAMPLE FACILITIES

Table 7-4 shows the average daily population (ADP) of the sample facilities. Table 7-5 breaks out the facilities by region and ADP. Table 7-4 shows that 40 percent of the total sample had an ADP under 500. Table 7-5 shows:

- The nine Northeast facilities were evenly distributed among small, medium, and large;
- Of the total of 14 institutions with an ADP of more than 1,000, 6 (43 percent) were located in the Midwest.
- The South and the Midwest each had 5 (36 percent) of the 14 institutions with ADP between 500 and 999.

Table 7-4
Average Daily Population

Population	n	%
Under 500	18	40
500-099	14	30
1000+	14	30
Total	46	100

Table 7-5
ADP by Region

Population	Northeast	South	Midwest	West	Total
Under 500	3	5	5	5	18
500-999	3	5	5	1	14
1000+	3	2	6	3	14
Total	9	12	16	9	46

Chi square analysis of the data used to develop Tables 7-4 and 7-5 reveals a nonstatistically significant relationship between size of a facility's average daily population and its location.* In other words, in terms of their size, the sampled institutions were randomly distributed.

* For four security levels, X^2 = 15.476; df=9; N.S. A comparison conducted without the "mixed" category, yielded X^2 = 8.247; df=6; N.S.

Survey Findings

SYSTEMS USAGE

Respondents indicated the types of MIS hardware and software being used at their facility.

Hardware

The number of different types of hardware cited for one institution ranged from 1 to 6 (the average was 2.9; the mode, found in 18 of the sample facilities, was 3). Table 7-6 shows that the most prevalent hardware used by respondents included wide area networks (WANs) (61 percent), mainframes (54 percent), and mini-computers (52 percent).

The list shown below displays, for each type MIS system, the kind of facilities in which it was ***least*** likely and most likely to be found. For example, wide area networks were least often used in moderate-sized institutions, in minimum security facilities, in older institutions, and in facilities located in the Northeast. WANs were most prevalent in small, new, mixed-security western facilities.

Table 7-6
MIS Hardware - Usage

	No. of Facilities	%
Wide Area Network	26	61
Mainframe	25	54
Mini-Computer	24	52
Micro-Computer	21	46
Local Area Network	17	37
NCIC - Dedicated Terminal	16	35

SYSTEM	USED LEAST OFTEN IN:	USED MOSTOFTEN IN:
WAN	Moderate-sized, minimum security, older facility, built in the Northeast	Small, mixed security facility, newly built in the West
Mainframe	Small, medium security, recently built facility in the South	Large, mixed security, older facility, built in the Northeast
Mini-Computer	Large, minimum security, old facility, built in the Northeast or West	Moderate-sized, maximum security, ancient facility, in the South and Midwest
Micro-Computer	Moderate-sized, medium security, new facility, built in the South	Large, mixed security, ancient facility, built in the West
LAN	Small, minimum security, ancient facility, built in the Midwest	Larger-sized, medium security, new facility built in the Northeast
NCIC-Dedicated Terminal	Small, maximum security, ancient facility, built in the Midwest	Largest, medium/mixed security, old facility, built in the West

Software

The average number of different software applications per institution was 23.4 (ranging from a high of 40 to a low of 11). These MIS software programs constituted three general categories: inmate programs, administrative/facilities support, and identification systems.

[Respondents were asked to indicate all that applied; therefore totals in the following sections will add to more than 100 percent.]

Inmate Programs. The 46 sample institutions reported using MIS software in four general inmate-related areas; the highest proportion of usage within each grouping was for the following:

Offender Case Management

- Admissions/releases - 96 percent
- Parole - 87 percent
- Classification - 78 percent

Inmate Activities

- Work assignment - 76 percent
- Education - 72 percent
- Movement control - 63 percent

Offender History

- Prior record tracking - 80 percent
- Detainers - 76 percent
- Medical/mental health records - 43 percent

In-Program Data

- Good time - 80 percent
- Disciplinary reports - 63 percent
- Grievance - 39 percent

Administrative/Facilities Support. Software programs in this category deal with management functions in a correctional facility. Under this heading the 46 sample institutions reported using software packages for four general activities. Among these the following four functions had the highest usage:

Accounting

- Payroll - 85 percent
- Accounts payable - 78 percent
- Purchasing - 72 percent

Personnel

- Leave status - 76 percent
- Training - 70 percent
- Staff scheduling - 50 percent

Inventory Control

- Supplied - 3 percent
- Equipment - 57 percent
- Perishable goods - 54 percent

Facilities and Operations

- Maintenance and scheduling - 43 percent
- Maintenance trouble log - 41 percent
- Food services - 39 percent

Identification Systems. Identification (ID) systems help prevent mistakes in identifying people-staff, inmates, and visitors. Respondents were asked to indicate which (more than one could be selected) of seven types of MIS inmate identification systems were in use at their facility. Three of the seven ID systems were not used by anyone-bracelet, retinal scan, and infrared. Level of usage by the sample facilities of the remaining four types was as follows:

- Picture ID card - 50 percent,
- Fingerprint - 22 percent,
- Bar code reader - 15 percent, and
- Magnetic card - 7 percent.

Only eleven (24 percent) of the respondents provided information concerning electronic identification systems. Because of the small number of replies, generalizations about these systems cannot be made. However, because the information provided by the 11 institutions might be helpful to a limited extent, it is reported separately at the end of this "Survey Findings" section.

CURRENT MIS TECHNOLOGY

All respondents (100 percent) agreed that MIS data was essential to the operation of their facilities. They were becoming increasingly dependent on computers. That was the good news.

The bad news was that in the average institution, MIS was not well managed. For instance, in 36 percent of the facilities responding, the various MIS application programs were not integrated with each other. That meant that general information had to be entered separately for each application.

Respondents were asked to list, in order of importance, the three MIS applications they considered most valuable. Responses fell into five categories. These are listed in Table 7-7, in order of their weighted, overall importance score.*

Table 7-7
Most important MIS Applications

	Score	%
Inmate-Related	132	51
Budget/Fiscal	57	22
Personnel	40	15
Word Processing	16	6
Other	16	6
Total	261	100

* Importance score = (the number of times a reply was listed first) x 3 + (number of times it was listed second) x 2 + (number of times it was listed third) x 1; i.e., each "first" listing = 3 points; each selection as a "second' choice = 2 points; and, each listing as a "third" choice = 1 point.

Over half the replies indicated inmate-related uses were the most important MIS applications; these out-weighed the second choice, budget/fiscal, by more than two to one. First-rated applications included inmate tracking and statistics, and classification.

In summary, most respondents were pleased with their inmate-related MIS programs. The 70 percent who considered these the most valuable applications (i.e., ranked them first), expressed needs for programs dealing with medical records, booking, classification, tracking, payroll, and accountancy applications.

Administrative applications were valued second after inmate-related applications. Twenty-two percent mentioned budget and fiscal applications as valuable.

Respondents also listed, in order of importance, three applications currently not automated that should be. Their replies fell into nine groups; these are listed in Table 7-8 in rank order (importance score is calculated the same as for Table 7-7).

Some of the applications listed were already in use at other facilities. Although happy with the inmate applications they had, administrators wanted programs for accounts, a fingerprint library, discipline, food service, grievances, housing rosters, inmate identification, medical, package deliveries, parole dates, personal property inventory, tracking good time, transportation schedules, and visitation records.

Table 7-8
Wanted MIS Applications

	Score	%
Inmate-Related	75	33
Staff -Related	32	14
Scheduling	26	11
Inventory	21	9
Maintenance	15	7
Food Service	14	6
Medical Services	11	5
Commissary	6	4
Other	25	11
Total	227	100

Among the wished-for business applications cited were programs for equipment and other inventories, a menu and recipe system, tracking budget line-items, check-writing, and general ledger. Personnel applications were also on the wish list, such as programs for labor relations activities, scheduling, leave, and payroll.

A few facilities did not have word processing and wanted it; others wanted to enhance their word processing capabilities with improved graphics and better ways to generate reports. Some wanted to be able to use the computer to schedule preventive maintenance. They wanted programs that were more responsive to local needs.

Generally, the reason for placing items on the wish list was to make the facility more efficient. The goal was to get accurate information more easily and make it more generally available. This would allow management to quickly respond to inquiries, spot trends, and make better informed decisions and more responsive plans. It would also reduce the space required to store paper reports.

In general, inmate-related programs were reported by the sampled institutions as both the ***must important*** MIS software applications - 51 percent of the replies---and the ***most wanted*** MIS programs - 33 percent endorsement rate.

INSTALLATION CONCERNS

Planning

Planning for MIS installations seemed more centralized than for other technological systems. Headquarters personnel were involved in planning MIS hardware in 56 percent of the facilities and in planning for software in 61 percent of the institutions. Staff had some say about hardware (30 percent of the facilities) and software (26 percent).

Several institutions turned to consultants for help with both hardware (26 percent) and software (22 percent), or involved the vendor in the planning (22 percent for hardware, 17 percent for software). In one facility, a National Institute of Corrections course helped in planning both hardware and software. Where planning was primarily done outside the institution, a facility staff member was involved in writing the specifications 85 percent of the time. In terms of who wrote the requirements, there was no significant difference between hardware and software*; for both, headquarters most often wrote the specifications.

Half of the respondents required performance bonds from the hardware installer, and 44 percent from the software vendor. When there was a performance bond, all the facilities required the bonded installer or vendor to fix any problems that arose.

Bugs

Although 56 percent of the respondents found no bugs when their hardware systems were installed, more than two-thirds (67 percent) had problems with software.? Hardware problems took a maximum of 3 months to resolve (average 3 to 6 weeks). For software problems the average time to solve these difficulties was 6 to 8 weeks. Only 9 percent used extra money to debug hardware; twice as many (18 percent) paid more than planned to debug software.

In summary, despite outside help, responses to the survey indicated that the sampled institutions were often disappointed with their information systems.

UNDERUTILIZATION CONCERNS

Regarding performance, 59 percent of the respondents believed hardware did ***nut*** meet all the needs of the facility, and 70 percent believed the same about their software. .§

More than three-quarters (76 percent) thought their MIS would be more responsive to their needs if a staff member had been involved in its development. Considering that, in the vast majority of cases, staff members were involved, they apparently were not given a large enough role or perhaps were not fully prepared to take one.

Given their frequent expression of disappointment with MIS, it was not surprising that fewer than half (49 percent) of the facilities reported optimal benefits, and 51 percent thought their system was underutilized.

* $X^2 = 0.792$; for df=6 N.S.

† However, this difference was not statistically significant; $x^2 = 3.6$; df=l; N.S.

§ The difference in level of dissatisfaction between hardware and software was not statistically significant; $X^2 = 1.245$; df=l; N.S.

Four potential causes emerged as reasons for the underutilization that was found: (1) lack of training; (2) a need to upgrade the system (so that the software would deal directly with the problems staff confronted regularly, and so there was enough equipment to meet staff needs); (3) nowhere to turn for problems with modified or customized software; and (4) shortage of onsite support Lack of training and upgrade needs were cited most often-by 57 percent of the respondents.

Lack of Proper MIS Training

The major themes in respondents' comments were:

- Without proper training, staff members were uncomfortable with computers and resisted using them,
- Their system had more applications than staff currently knew how to use, and
- Facilities lacked the money to upgrade their personnel's skills.

When asked which staff positions should be trained to use MIS systems, the 44 responses received fell into the seven groups shown in Table 7-9. Line officers and support staff (e.g., storekeepers, business office) were the personnel seen most as being in need of MIS training.

Table 7-9
Who Should Be Trained?

	%
Line Officers	23
support staff	20
Administrators	16
Supervisors	16
Program Personnel	16
All Staff	5
Clerical	2
Total	100

Insufficient Upgrades

The need to upgrade MIS stemmed from a different set of difficulties, though once again lack of funds was a factor. Major problems cited were that software formats were not flexible enough to meet current demands, and there was not enough hardware to service all the staff needing to use the system.

Fifty-nine percent of the facilities had user groups (a.k.a. automation committees) that evaluated the need for system modifications. Respondents listed, in order of importance, three factors they considered when MIS upgrades were contemplated. The 99 responses received fell into six groups, listed in Table 7-10 in order of their overall importance score (calculated the same as for Table 7-7).

Table 7-10
MIS Upgrade Considerations

	Facilities	%
cost	81	34
Central Office Decision	42	18
Need	39	15
Software Availability	30	13
Down-Time	20	8
Other	28	12
Total	240	100

Cost of the potential upgrade far out-weighed other factors in importance-almost twice as high as the next consideration-when an MIS upgrade was contemplated.

Seventy-six percent of the respondents had upgraded their hardware, and 86 percent installed new software. Four institutions (11 percent) reviewed and upgraded their hardware systems once a year; 34 others followed a random schedule. In regard to software, 35 respondents reviewed their programs on a random timetable.

Software Modifications

Software used in the responding correctional facilities was often modified after it came from an outside vendor. Although only 7 percent of the respondents used software written specifically for their institution, 66 percent had software that was customized to meet their own needs; 55 percent had modified off-the-shelf software. However, when problems arose with customized software, institutions had nowhere to turn for assistance except to their own staff or consultants.

Support Staff

The replies also suggested a shortage of onsite support for staff members using MIS. Only 46 percent of the responding facilities had someone on hand to solve hardware difficulties, while 47 percent had someone to answer questions about software. Among institutions not currently offering support, more than seven out of ten (69 percent) believed onsite support would help.

OPERATIONAL CONCERNS

Staff Training

Staff who used MIS were required to be computer-literate beforehand in just over a third (35 percent) of the responding facilities. Training, however, was not universal: 89 percent instructed staff on hardware usage and 96 percent on software. For the former, the average number of training hours was 7 (ranging from a high of 40 to a low of 1 hour). Software training was at least twice as long, 15 hours on average, with the range again from 1 to 40 hours.

Often the length of training depended on what the staff member already knew, the particular software application, and on how fast an employee learned. Thus, high quality MIS training for staff was not guaranteed (e.g., one institution indicated that its hardware training was limited to ***"being shown what to do by a fellow staff member").***

Research for this project suggests that institutions often got outside training assistance for their personnel in other correctional technologies. This seemed to be less true for MIS training. Most often (76 percent) there was in-house support specifically for MIS training. In almost six out of ten cases (59 percent), the facility took that responsibility. Sometimes (28 percent) the MIS application had a tutorial which could train staff. Facilities that sought outside training went to vendors (27 percent) and to other organizations like the state training academy, the division of state police, or a community college.

Once trained, staff members needed to be kept current. Reportedly, keeping up-to-date was less likely for hardware than for software.

Almost all institutions provided MIS training to administrative (98 percent), clerical (96 percent), and support staff (85 percent).* Line officers were also likely to be trained (54 percent). Systems implementation was much easier when top administration was both computer-literate and committed to automation.

The average number of staff who received MIS training was low (only 23 percent, although the range was from 1 percent to 84 percent). More than four out of ten facilities (47 percent) recognized the need to train other staff, among them security supervisors, upper-level supervisors, program staff who tracked inmates, case managers, medical staff, maintenance staff, mental health counselors, and classification staff.

Computer Security

In two out of three facilities (67 percent), inmates' assignments did not require them to use computers; 98 percent of the facilities did not permit inmates to be involved in the repair or maintenance of hardware.

Ninety-one percent of the respondents had written policies to protect the security of their MIS hardware and software. The following were among the topics covered in these policies:

- Data backup procedures (listed in 92 percent of the replies),
- Inmate access to, and use of, computers (90 percent),
- Frequency of backups (89 percent),
- Software documentation (86 percent),
- Staffs personal use of computers (77 percent),
- Storage of backups in-house (77 percent) or elsewhere (52 percent), and
- Archive procedures (72 percent).

Computer security policies and procedures should be centrally coordinated. The Federal Bureau of Prisons recently established a computer security officer within in its headquarter's Office of Information Systems. This individual is responsible for implementing, directing, and monitoring the Bureau's overall computer security programs.

The respondents indicated that MIS security was not often compromised. Only five institutions had problems during the year prior to the survey. One prisoner was allowed to use the system without authorization, another inmate gained access to the applications' operating system (DOS) by by-passing the security program through a WordPerfect shell, and staff members used data for nonwork-related reasons or used the system for personal activities.

Actions taken by the affected facilities included termination of the miscreant staff member, better supervision, and modification of the user-identification system to better control access.

About a third (32 percent) of the facilities reported having an automation officer who was responsible for keeping MIS secure. Among other staff given such responsibility were users (in 33 percent of cases) and security (10 percent).

REPAIRS AND MAINTENANCE

Keeping the MIS hardware up and running was a staff responsibility in 61 percent of the reporting facilities. Staff members given this assignment included an automation coordinator, other

* These figures differ from those in Table 7-9, which deals with who needed to be trained, as opposed to who actually received training.

in-house computer specialists, a member of the central maintenance support unit or the data processing unit, someone in maintenance services, or someone in the central office of the department of corrections.

More than half (54 percent) of the facilities had MIS maintenance contracts, 17 percent depended on other outside contractors, 13 percent on the vendor, and 7 percent on the manufacturer. Only a few facilities (13 percent) trained their own personnel to maintain MIS hardware. In those instances, the staff member trained was usually a computer repair specialist; others trained were the system administrator, an MIS liaison, an institution automation officer, computer support staff member, or employees particularly skilled in using computers.

In one out of three cases (35 percent), maintenance training was provided in-house; sometimes (27 percent) it came from the vendor. Other resources for training included the central office data center, an employee with specialized training, or the local community college.

Preventive maintenance was a priority for only about one out of four (27 percent) facilities; the others report no preventive maintenance program. For those that did have scheduled maintenance, down-time per year averaged 133 work-hours (ranging from 572 to as low as 20 hours).

Unscheduled repairs, which were reported by 29 facilities, kept information systems down for as long as 6 weeks-five facilities reported an average down-time of 4 weeks, another eight averaged 4 days, and 14 averaged 23 hours.

Where staff was responsible for repairs, most facilities were satisfied with the arrangement; only 31 percent thought a maintenance contract would cut the cost of repairs, while 43 percent thought a contract would improve the quality of repairs.

Other enhancements used to keep MIS operating and effective included automated back-up for the system (38 percent of respondents) and an uninterrupted power source (46 percent); although one facility noted that the power source was uninterrupted only for the headquarter’s mainframe, but not for the institution’s mini-computer.

For most systems (84 percent), spare parts were readily available from the factory or a dealer. Consequently, 93 percent of the respondents did not store spare parts.

IDENTIFICATION SYSTEMS

This description of identification (ID) systems is placed at the end of this section because of the small number of responding institutions in which it was being used: Only 11 (24 percent) of those sent survey questionnaires were using ID systems. Because of this small number of respondents, generalizations about these systems cannot be made; however, it is believed that the experiences of these 11 institutions might be helpful to a limited extent.

Although 78 percent of the facilities responding to the survey believed that an ID system would improve security, only 11 facilities actually had this technology. One had such a system for 17 years and one for only 6 months; the other nine electronic ID systems had been in place for an average of about 8 years.

ID systems were installed to solve some particular problem, such as improving security, improving accountability, or in one case, removing money transactions from the institution and, thereby reducing pressure from inmates. All respondents agreed that their systems solved the problem for which it was installed.

Uses

All 11 institutions used their ID system with staff; 10 also used it for inmates; 4 used it with visitors. When used for prisoners, the ID system tracked movement outside and within the institution, commissary purchases, visits, infirmary cases, library use, or, in one instance, inmate pay verification.

Security

Ten of the 11 responding institutions (91 percent) indicated that their ID systems were essential for security. Its absence, they said, would have increased the possibility of escapes; given inmates access to information they should not have; caused staff to misidentify inmates and/or visitors and to confuse both; and in mixed facilities, would have made it difficult to determine the custody level of an inmate.

There was unanimous agreement among the respondents that their ID systems prevented mistakes in identifying people. ID systems were considered sufficiently sturdy and tamper-resistant by 8 of the 11 facilities, but one respondent indicated that its system could use a stronger and more adhesive plastic seal. Another believed its ID system could be better integrated with other management information systems.

Only one respondent reported an ID system being compromised; an inmate altered his badge and walked out with a construction crew. In response, the facility increased training for staff at exit points.

ID System Procedures

IDs were changed either when a person's appearance changed, at go-day intervals, when an ID was lost, or when someone joined or left the staff or was promoted.

Identification systems for staff were rarely integrated with other systems, like key and tool control, or hand-held radios.

Installation

There were bugs in the ID system at first in three of the facilities, but all were corrected within a month, most without additional cost.

Although one institution installed its ID system without establishing written specifications, generally, stipulations were likely to be written by users [e.g., headquarters (36 percent), facility staff (27 percent), DOC automation officer (9 percent)]. Vendors and consultants wrote specifications for some installations; often no performance bond was required.

Training

Where staff members were responsible for maintenance, the average number trained was three, most likely either a line officer or a technician, but in some cases other certified employees (e.g., records and identification staff, supervisors, or office automation specialists).

Only one out of four respondents had an ongoing program to train new staff and to maintain the proficiency of experienced personnel. The training itself was usually provided by the facility (75 percent), though sometimes by the manufacturer (25 percent).

Maintenance, Repairs, and Testing

Responsibility for keeping the ID system in good repair usually rested outside the institution, with the manufacturer (36 percent), a maintenance contractor (18 percent), or other outside contractor (9 percent). Staff were primarily responsible for maintenance and repair in only three institutions. That may explain why only two facilities trained their own staff to maintain the ID system; one provided 8 hours of training and the other 40 hours.

Only three institutions found it necessary to test their ID systems regularly, one quarterly and the other two at random intervals. Staff were expected to identify problems and report them to the vendor. As two respondents commented, because the ID system was used daily, glitches were likely to be recognized promptly even where there was no scheduled testing. In any case, all the reporting institutions considered their electronic ID systems to be tamper-proof.

Down-time for unscheduled repairs was rare; one ID system was down for a week and another for 3 days. In the three institutions that had scheduled maintenance, the system was down for a high of 200 hours and a low of 4. As with other management information system technology, ID systems could be repaired during off-hours.

Only three institutions stocked spare parts for key components of their ID systems, because 78 percent of the facilities could get spare parts easily from the factory or dealer.

Conclusions and Issues

CONCLUSIONS

Correctional administrators agreed that information systems were critical to the efficient operation of their facilities, but many (51 percent) believed they were not benefiting all they could from MIS. Some thought their systems were too sophisticated for the personnel; for several others the prime concern was dealing with staff fear and resistance to change. Still others had to overcome outdated systems (26 percent), not enough equipment (22 percent), or a lack of integration among the applications they must use (13 percent). A common dilemma was summed up as follows:

> ***Several departments use personal computers with nationally advertised programs which perform the functions required. The business office works off a mainframe used by all state agencies for purchasing. It seems we really have two MIS systems. Everyone with a PC does his or her own thing.***

In general, local applications were less likely to be integrated. Linking PCs with one another into local area networks (LANs), seemed to have low priority.

Hardware

Over half of the respondents indicated that they have at least one of the following three types of MIS hardware:

- Wide area network (WAN),
- Mainframe, and
- Mini-computer.

WANs were most frequently reported as being in small, newly built, mixed security institutions, located in the West. Mainframes were most often reported in large, mixed security, older facilities, built in the Northeast. Moderate-sized, ancient, maximum security institutions in the South and Midwest most often housed mini-computers.

Software

The average number of software programs per institution was 23.4 - ranging from a high of 40 to a low of 11. These fell into three general categories: inmate-related programs, administrative/ facility support, and identification systems. For each category, the most widely used applications were:

- Inmate-related applications-offender case management
  - Admission/Release programs (used by 96 percent of respondents),

  - Parole-related (87 percent), and
  - Classification programs (78 percent).

- Administrative applications-accounting
  - Payroll (used by 85 percent of the respondents),
  - Accounts payable programs (78 percent), and
  - Purchasing-related programs (72 percent).

- Identification systems (used by only 24 percent of respondents)
  - Picture ID (50 percent of those with an ID system),
  - Fingerprint (22 percent), and
  - Bar code reader (15 percent).

Training

Of the facilities that lacked trained staff, five reported no onsite user support for either hardware or software. Among the managers that believed their MIS was underused, 70 percent did not require staff using the system to be computer literate despite the fact that 56 percent of them recognized that lack of training caused problems. Additionally, these managers recognized the importance of training administrators and supervisors. One commented:

> ***System implementation is much easier when top administration is computer-literate and committed to automation. Special effort should be made to properly train line supervisors so that they understand and can explain to subordinates the purposes and usefulness of MIS systems. Emphasize the efficiency and benefits of automation and provide adequate training and support to minimize anxiety among staff who are not computer-literate.***

Personnel were trained an average of 7 hours on hardware and 15 hours on software; even this appeared to be haphazard (e.g., basing the training on the trainees' previous knowledge).

A further complication resulted from training being provided by individuals who were not specialists but by other staff members who had an interest in MIS. Moreover, once the initial session was completed, more than 60 percent of the facilities provided no refresher training.

There was a relationship between who did the training and how well the system was used. Institutions reporting MIS underutilization were also the ones who did training in-house (87 percent). The fact that someone is comfortable and even enthusiastic about MIS did not automatically make that person an effective instructor. The ability to use a system did not necessarily mean having adequate knowledge or being able to teach others about all of its capabilities. Although satisfied with their own skills, these individuals did not know the most effective ways to use the system and its applications.

In addition to training deficiencies, institutions with underused systems also lacked onsite support. Another facility recommended that this problem be taken into account from the beginning:

> ***Reference documentation should be provided [when installing a new management information system] so the users may refer to it when questions arise, rather than having to send memorandums or place telephone calls hoping to locate an answer.***

Facilities with underutilized systems were also likely to upgrade randomly (70 percent). They had no user groups to evaluate new systems (55 percent), were more likely to cite cost (45 percent) as a factor when choosing a system rather than need (22 percent), and rarely involved staff in developing specifications for either hardware or software (26 percent).

ISSUES

Information received from the survey's respondents highlight several reasons for the underutilization of management information systems. Two of the most significant are that administration tended not to consider the human element in MIS systems, and there was a lack of clearly stated objectives that the system was to address.

The most important component in a management information system is the people who use it. The need for the system stems from problems within the organization and the requirements of staff. System planning needs to incorporate both elements into the design process.

MIS is only as good as the help it provides. Consequently, initial cost-always a significant factor in a purchase or upgrade decision--cannot be the sole justification. The base questions are:

- What do we want to do with the system?
- Who will be using it? and
- What other systems must it communicate with?

For new institutions, planning for MIS must be part of the master strategy. All administrators should think through both short- and long-term requirements, not only in the individual facility, but also for the department as a whole. Among factors that must be considered are cost, software availability, training, flexibility and compatibility, maintenance, staff support, and security.

Cost

It is necessary to look beyond the initial purchase price of a new information system and to project total life-cycle costs involved in its operation, maintenance, and upgrading. For example:

- What are the direct and indirect costs of scheduled maintenance?
- How easily and cheaply can replacement parts be obtained?
- How quickly and efficiently can staff be taught to use it?

Software

Potential users are the best source of information for planning software acquisitions. Questions to be considered, include:

- Are there off-the-shelf packages available that will do the job?
- If software must be customized, will it be compatible with programs already in use so that information entry need not be duplicated?
- What support (assistance) is available for software users?
- How flexible is the package, and what will it cost to upgrade?

Training

Respondents made it clear that information systems were only as effective as the people who used them. Potential users should be consulted early in the MIS design process so that after the system is in place it will meet their needs.

Additionally, both initial and follow-on training need to be planned, so staff will know how to make MIS do what they want it to. Familiarity breeds comfort.

The planning process should address several questions about training ***before the*** decision about which system to use is made:

- What training packages are available?
- How well do they work?
- Who will be trained initially and later?
- Who will conduct the training?
- Can the training program be adapted to individual needs and abilities?

Flexibility and Compatibility

Information systems must be versatile and adaptable. Important considerations relate to how well MIS supports (1) administration, (2) inmate programs and management, and (3) inmate and other types of identification. Questions should include the following:

- Can the system be used in inmate education programs?
- Can it be adapted to incorporate changes in the physical plant?
- Should it include modem and facsimile transmission capability?
- Should it include such features as E-mail or executive scheduling?
- Will it link all the computer options currently available-not just in the facility but across the state or federal jurisdiction?
- Can it be incorporated into a local or wide area network?
- Can it be integrated with voice communication systems if that seems advisable?
- Which current systems can it incorporate, and which can it replace?

Maintenance

Should maintenance be handled onsite or through a contract? What are the advantages, disadvantages, and costs of each option? What must be included in preventive maintenance and can it be done during off-peak hours? If maintenance is to be done onsite, how will staff be trained? How much will parts inventory cost not just to buy but also to store?

staff support

Is it advisable to have dedicated training staff? Maintenance staff? Programmers? Systems analysts? Troubleshooters? In-house consultants for applications problems?

security

Will the physical plant have to be modified to protect MIS hardware? How will data be stored so that it will be protected? Who will have access to which files?

Additional Issues

A major reason for the failure and/or misdirection of system planning efforts was the reluctance of the system users to challenge suggestions made by top management. The team developing the

MIS system should include specialized personnel who understand the problems to be solved (from both management's and users' perspectives) and can provide guidance as to whether or not proposed solutions will work. The development team should address the following:

1. Consider whether or not the system will meet the facility's projected information needs for the next 5 years.

2. Determine precisely what current problems the MIS technology should resolve.

3. Avoid confusing system objectives with system development objectives.

4. Consider what type of users are to be served.

5. Determine if there are subgroups of users who have needs that differ from those of the general staff.

6. Contact other users of the equipment to be purchased to benefit from their experience.

7. Purchase equipment for which parts will be readily available, and will remain available, once the system is installed and for which there are local contractors who can provide 24-hour service.

8. Determine whether or not the system has a good warranty and is explicit as to what is covered.

9. Develop a plan for onsite hardware and software support.

10. Request that the vendor provide detailed documentation of the system.

11. Obtain schedules for maintenance and repair from the manufacturer, vendor, and/or installer and a schedule for (and information on) appropriate testing methods.

12. Determine whether or not maintenance and repair of the system will be accomplished by facility staff or by a maintenance contract.

13. Specify the amount and type of training. Sound training employing modem technology requires a long lead time; therefore, start training as early as practicable. Plan for staff to be trained in how to operate, maintain, and repair the system. Try to arrange the training as part of the sales contract.

14. Decide the level of staff that will be trained and ensure that it includes management as well as support staff.

15. Plan how follow-on training will be provided for both present personnel and new hires.

16. Consider whether or not this effort is a result of the desire to use a modem computer system for its own sake (i.e., Is it really needed?).

Chapter 7

Questionnaire Data-Management Information Systems

47 Responses

Mainframe Computers	25	Micro-Computers	21
Mini-Computers	24	NCIC Terminals	16
Local Area Networks (LANs)	17	Wide Area Networks (WANs)	28
Identification (ID) Systems	11	Other (specify)	3

Administrative and Facilities Support Functions

Place an (x) alongside AU types of applications available on your management information system.

Accounting		Inventory Control	
Accounts Payable	78	Equipment Inventory	36
Accounts Receivable	67	Perishable Goods Inventory	25
Payroll	85	Supplies Inventory	27
Purchasing	72	Other (specify)	5
Billing	57		
Statistical Reporting	70		
Trust Accounting	61		
Inmate Welfare Fund	59		
Other (specify)	5		

Personnel Status		Facilities & Operation	
Staff Scheduling	23	Food Services	18
Training	32	Maintenance and Scheduling	20
Leave Status	35	Maintenance Trouble Log	14
Career Development	10	Medical/pharmacy Services	16
Performance Record	9	Clothing/Linen Tracking	12
other (specify)	4	Laundry	6
		Other (specify)	1

Inmate Programs

Inmate Programs		Offender Case Management and History	
Community Service	10	Admissions/Releases	44
Work Release	16	Parole	40
Correspondence/Visits	14	Detainees/Holds	35
Victim Restitution	15	Biographical/Demographic Classification	36
Movement Control	29	Personal Property Control	8
Prison Industry	16		

Inmate Programs (can't)	
Educational	33
Training	20
Work Assignment	35
Counseling	14
Other (specify)	5

Offender Case Management and History (can't)	
Grievances	19
Disciplinary Actions	29
Reclassification/Review Information	31
Medical/Mental Health Records	20
Prior Arrest/Prior Criminal Record Tracking	37
Good Time	37
Other (specify)	3

Communication Networks with Law Enforcement	
County	8
State	25
Federal (NCIC)	19
Other(specify)	4

Identification	
Bar Code Reader	7
Bracelet	0
Fingerprint	10
Retinal Scan	0
Magnetic Card	3
Picture ID Card	23
Infrared	0
Not Applicable	10
Other (specify)	6

Hardware/Software

1. Is the management information system (MIS) essential to the operation of this facility?
Yes 46 No 0 Don't Know 0

2. What would be the effect on the operation of this facility if the MIS was removed? (covered in text)

		Yes	No	Don't Know
3.	Are the MIS applications integrated? (e.g., general information needs to be entered only once)	29	16	1
4.	Is the system standardized for all work stations in this facility?			
	Hardware	46	12	**0**
	Software	37	9	**0**
5.	Is the system standardized for all facilities in this department of correction?			
	Hardware	31	13	2
	Software	34	11	1
6.	Can the system be upgraded/expanded to meet future needs?			
	Hardware	41	12	4
	Software	42	1	3

	Yes	No	Don't Know
7. Has the system ever been upgraded?			
Hardware	31	10	5
Software	37	6	3

8. How often is the system upgraded?

	Hardware	Software
Times Per Month	0	0
Times Per Year	0	0
Randomly	37	35

9. What factors are considered in determining whether the system is upgraded (e.g., availability of software/hardware, cost, downtime)? Please list them in order of importance with #l being the most important. (covered in text)

10. The specifications for the system were written by [Check (x) ALL that apply]:

	Hardware	Software
Facility Staff	14	12
Consultant	12	10
Vendor	10	8
state Staff	24	26
Automation Office Staff	10	12
National Institute of Corrections	1	1
There were no specifications.	1	1
Other (specify)	2	2

	Yes	No	Don't Know	No Response
11. Was a performance bond required of the supplier/vendor/installer of the system?				
Hardware	5	5	0	0
Software	4	5	0	0
12. If yes, was the supplier/vendor/installer held to the performance bond?				
Hardware	4	0	25	17
Software	4	0	24	18
13. If specifications were produced by someone other than staff, was there a staff member involved in writing the specifications?	17	3	20	6
14. Does the system meet all of the needs of the facility?				
Hardware	18	26	2	0
Software	13	31	2	0
15. If no, do you believe that the applications would be more responsive to the needs of the facility if a staff member had been involved in their development?	14	6	2	19

16. The management information system currently [Check (x) ONE]:

Provides optimal benefits for the institution	22
Is underutilized	23

17. If the system is underutilized, what is the reason? (covered in text)

		Yes	No	Don't Know	No Response
18.	Does the facility have support services onsite to answer questions and solve problems for staff?				
	Hardware	21	25	0	0
	Software	21	24	0	1
19.	If no, do you believe that if onsite support services were available staff would make more efficient use of the management information system?	18	8	1	19

20. Was the software [Check (x) ONE]:

Written specifically for the use of this facility	3
Purchased off the shelf	12
A combination of both	29
No Response	2

		Yes	No	Don't Know	No Response
21.	If the software was purchased off the shelf, was it modified for use in this facility?	16	13	10	7
22.	Did the facility experience bugs in the system after installation was complete?				
	Hardware	16	20	10	0
	Software	24	12	10	0

23. If yes, for how long? (covered in text)

		Yes	No	Don't Know	No Response
24.	Were additional funds required to debug the system?				
	Hardware	2	20	19	5
	Software	4	18	20	4

		Yes	No	Don't Know	No Response
25.	Are staff who use the MIS system required to be computer literate before they use it?	16	30	0	0
26.	Is training provided for staff to learn how to use the management information system?				
	Hardware	41	5	0	**0**
	Software	44	2	0	**0**

27. How many hours of training are required for staff to learn to operate the MIS system?

Hardware		Software	
# of Responses - 26		# of Responses - 28	
Average # of Hours - 7.27		Average # of Hours - 14.57	
High 40	Low1	High 40	Low 1

		Yes	No	Don't Know
28.	Is there an on-going program to keep all staff proficient on the system as well as train new staff?			
	Hardware	22	24	**0**
	Software	24	21	1
29.	Is there a user work group/ automation committee that evaluates new systems (i.e., hardware, software, modifications)?	23	16	

30. Which staff are trained to operate the system? [Check (x) ALL that apply.]

Line Officers	25
support Staff	39
Administrative	45
Clerical	44
Plant Operations	14
Other (specify)	6

31. What percentage of staff are trained to operate the management information system?
# of Responses - 46 Average - 22.63% High 84 Low 0.60

32. Are there additional staff positions that should include training to operate of the system?
Yes 20 No 26

33. If yes, which other staff positions should include training to use the management information system? (covered in text)

34. The training is provided by [Check (x) ALL that apply]:

Vendor	10
Manufacturer	1
Facility	27
Video	6
Computer-Based Tutorial	13
In-House Support Services	35
other(specify)	13

		Yes	No	Don't Know	No Response
35.	Are inmates assigned job responsibilities that require access to computers?				
	Data-related jobs	15	31	0	0
	Maintenance and repair of hardware	1	45	0	0
36.	Are there policies established to maintain the security of the management information system?				
	Hardware	41	4	1	0
	Software	41	**4**	1	0
37.	Do the policies regarding the management information system include (Answer ALL of "a" through "h"):				
	a. Data Backup	34	**3**	4	**5**
	b. Frequency of Backups	31	**4**	6	**5**
	c. Storage of Backups In-house	27	**8**	5	**6**
	d. Storage of Backups Away from Institution	17	16	7	**6**
	e. Archives	23	9	9	**5**
	f. Personal Use of Computers	30	9	2	**5**
	g. Inmate Access and Use of Computers	36	**4**	1	**5**
	h. Documentation of Software	25	4	12	**5**
38.	Has the security of the system been compromised at any time within the last year?	4	32	10	

39. If yes, what were the circumstances? (covered in text)

40. What was done to correct the situation? (covered in text)

41. Who is responsible for system security?

Institution Automation Officer	14
Other (specify)	30

42. Who is responsible for maintenance and repair of the hardware? [Check (x) ONE.]

Staff	16
Vendor	6
Manufacturer	3
Maintenance Contract	25
Outside Contractor	8
Other (specify)	12

43. If staff has maintenance responsibilities, does the facility have an established training class in which staff learn to maintain and repair the hardware?
Yes 3 No 21 No Response 22

44. Which staff are trained to maintain and repair the hardware? [Check (x) ALL that apply.]

Line Officers	0
Computer Specialists/ Repair Personnel	18
Other (e.g., line, support staff, etc.)	9
No Response	19

45. Does the facility have an established preventive maintenance program for the hardware?
Yes 10 No 27 Don't Know 6 No Response 3

46. The training is provided by [Check (x) ONE]:

Vendor	7
Facility	9
Other (specify)	10
No Response	20

47. What is the average amount of down-time per year for unscheduled repairs and preventive/scheduled repairs? (covered in text)

	Yes	No	Don't Know	No Response
48. If staff now perform maintenance/repairs, do you believe a maintenance contract would be an improvement?				
a. For Cost	4	9		24
b. For Quality of Repairs	6	8		24

		Yes	No	Don't Know	No Response
49.	Does the system have automated back-up?	11	18	15	2
50.	Is the management information system on an uninterrupted power source?	18	21	7	0
51.	Does the facility stock spare parts for key components of the system?	3	39	4	0

52. Are spare parts readily available from the factory or dealer?
Yes 26 No 5 Don't Know 12 No Response 3

53. List the three applications you consider to be the most valuable. Please list in order of importance, #l being the most important (covered in text)

54. List the three applications that are currently not automated that you believe should be. Please list in order of importance, #l being the most important. (covered in text)

55. How would these applications make your management information system more efficient or effective? (covered in text)

Automated/Electronic Identification (ID) Systems

1. Do you believe that an ID system would improve security at this facility?
Yes 28 No 8 No Response 10

2. An ID system has been used in this facility for how long?

# of Responses - 8 Average # of Years - 7.88 High 17 Low 3
# of Responses - 3 Average # of Months - 7.33 High 10 Low 6
Don't Know 1 Other 0

3. The ID system is used for [Check (x) ALL that apply]:

Staff	11
Inmates	10
Visitors	4
Vendors	3
Other (specify)	2

4. Does the ID system document use of the following areas for staff and/or inmates? [Check (x) ALL that apply.]

	Inmates	Staff
Library	1	0
Infiiary	2	0
Commissary	6	0
Visits	5	1
Movement Outside of Institution	7	4
Movement Through Institution	5	2
Other (specify)	1	0

5. Is the ID system essential to the security of the facility?
Yes 10 No 1 Don't Know 0

6. What would be the effect on the security of this facility if the ID system was removed? (covered in text)

7. Does the ID system prevent mistaken identities?
Yes 11 No 0 Don't Know 0

8. Is the ID system sturdy and tamper-resistant?
Yes 8 No 3 Don't Know 0

9. If no, how can it be improved? (covered in text)

10. Did the facility experience bugs in the system after installation was complete?
Yes 2 No 7 Don't Know 2

11. If yes, for how long?

# of Responses - 0 Average # of Days - 0	# of Responses - 1 Average # of Weeks - 1
# of Responses - 1 Average # of Months - 2	# of Responses - 0 Average # of Years - 0

12. Were additional funds required to debug the system?
Yes 2 No 5 Don't Know 2 No Response 2

13. The specifications for the ID system were written by [Check (x) ALL that apply]:

Facility Staff	3
Consultant	2
Vendor	3
State Staff	4
Department Automation Officer	1
There were no specifications.	1
Other (specify)	2

		Yes	No	Don't Know	No Response
14.	Was a performance bond required of the supplier/ vendor/installer?	1	3	6	1
15.	Was the supplier/vendor/ installer held to the performance bond?	1	3	6	1

16. Who is responsible for the maintenance and repair of the ID system? [Check (x) ALL that apply.]

Staff	3
Manufacturer	4
Maintenance Contract	2
Outside Contractor	1
Other (specify)	3

17. If staff, does the facility have an established training class in which staff learn to maintain and repair the ID system?
Yes 0 No 7 No Response 4

18. How many hours of training are required for staff to learn to maintain and repair the ID system?
# of Responses - 2 Average # of Hours - 24 High 40 Low 8

19. How many staff members are trained to maintain and repair the ID system?
# of Responses - 6 Average # of Hours - 2.83 High 6 Low 2

20. Which staff are trained to maintain and repair the system? [Check (x) ONE.]

Line Officers	3
Technicians	3
Other (specify)	4

21. Is there an on-going program to train new staff and keep all staff proficient on the system?
Yes 2 No 6 No Response 3

22. The training is provided by [Check (x) ONE]:

Vendor	0
Facility	3
Manufacturer	1
Other(specify)	0

23. What is the average amount of down-time per year for scheduled repairs and preventive/scheduled maintenance? (covered in text)

		Yes	No	Don't Know	No Response
24.	If staff now performs maintenance/repairs, do you believe a maintenance contract would be an improvement?				
	a. For Cost	1	2	5	3
	b. For Quality of Repairs	2	2	4	3
25.	Does the facility have an established preventive maintenance program for the system equipment?	1	6	2	2
26.	Does the facility stock spare parts for key components of the system?	2	6	3	0
27.	Are spare parts readily available from the factory or dealer?	7	2	2	0

28. How often is maintenance/testing performed on the ID system and what does it involve? [Check (x) ALL **that apply.]**

weekly	0
Monthly	0
Quarterly	1
Semiannually	0
Annually	0
Randomly	2
Other (specify)	2

29. Who performs the scheduled maintenance/testing and what are they responsible for? [Check (x) ALL that apply.]

Staff	2
Vendor	1
Outside Contractor	0
Other (specify)	0

30. Has the ID system remained as tamper-resistant as when it was installed?
Yes 8 No 0 Don't Know 2 No Response 2

31. If no, what steps have been taken to make the system tamper-resistant? (covered in text)

32. How often are IDs changed?

Every Shift	0
Daily	0
weekly	0
Other (specify)	9
No Response	2

33. Has the ID system ever been compromised?
Yes 1 No 7 Don't Know 3

34. If yes, what were the circumstances? (covered in text)

35. Did this jeopardize the security of the facility?
Yes 1 No 1 Don't Know 2 No Response 7

36. What was done to correct the situation? (covered in text)

		Yes	No	Don't Know
37.	Is the staff ID system integrated with key control?	2	8	1
38.	Is the staff ID system integrated with tool control?	**1**	9	**1**
39.	Is the staff ID system integrated with hand-held radios?	**1**	9	**1**

		Yes	No	Don’t Know
40.	Was the ID system installed for a particular reason or to solve a specific problem?	7	2	2

41. If the ID systems was installed for a specific reason, what was that reason? (covered in text)

42. Has the ID system met expectations in terms of solving that problem?
Yes 6 No 0 Don’t Know 1 No Response 4

43. If it has not solved the problem, why? (covered in text)

Appendix: Resource Materials

Bare, William K. “Fundamentals of Fire Prevention.” New York, 1977.

Benton, F. Warren, and Robert Obenland. “Prison and Jail Security.” Washington, D.C.: U.S. Department of Justice, Law Enforcement Assistance Administration, 1973.

Camp, George, and Camille Camp. “Stopping Escapes: Perimeter ***Security.” Construction Bulletin*** (March 1987).

Cohen, Susan B. “Never Forget . . . Behind Every Good Security System Stand the People Who Make It Work.” ***Corrections Today 53*** (July 1991).

Communication Equipment and Engineering Company, Plantation, Florida.

Cunningham, John E., and Delton T. Horn. “Handbook of Remote Control & Automation Techniques.” 2nd edition. TAB Books, Blue Ridge Summit, Pennsylvania, 1984.

Del Norte Security Systems, Division of Southwest Microwave, Inc., Tempe, Arizona.

Dewar, Michael. “Weapons & Equipment of Counter-Terrorism.” London, 1987.

Dictaphone Corporation, Stratford, Connecticut.

EG&G Astrophysics Research Corporation, Long Beach, California.

Elm, William R. “Rapid-Response System Boost Safety and Control.” ***Corrections Today 52*** (July 1990).

Fike, John L., and George E. Friend. “Understanding Telephone Electronics.” Dallas, 1984.

Finneran, Eugene D. “Security Supervision: A Handbook for Supervisors and Managers.” Boston, 1981.

Folger Adam Company, Lemont, Illinois.

Freeman, Ira M. “Physics Made Simple,” revised edition. New York, 1990.

Gateway Technologies Inc., Dallas, Texas.

Garrett Security Systems, Inc., Garland, Texas.

Graf, Rudolph F. "Modem Dictionary of Electronics." New York, 1972.

Green, Gion, and Raymond G. Farber. "Introduction to Security-Principles & Practices," revised edition. Los Angeles, 1979.

Hahn, Steven. "Modem Electronic Security Systems." Rochelle Park, New Jersey, 1976.

Harris Corporation, Digital Telephone Systems Division, Novato, California.

Hill, Bryan L. "Staff Training. Mastering Security Technology." ***Corrections Today 53*** (July 1991).

Intellicall, Inc., Carrollton, Texas.

International Business Machines Corporation, Rye Brook, New York.

Jameson, Robert, and Charles Megerman. "Automation in a Medium-sized Jail." ***Corrections Today 52*** (July 1990).

JWP Electronic Systems, Purchase, New York.

Kevorkian, Harold H. "An Internship with the Safety Department of the United States Penitentiary, Leavenworth, Kansas." Northwestern University, 1968.

Kirk, Frank G. "Total System Development for Information Systems." New York, 1973.

Latessa, Edward J., et al. "Impact of Technology on Adult Correctional Institutions." Cincinnati: University of Cincinnati, July 1988.

Libolt, Adria Lynn. 'Technology Cannot Be a Replacement for Creative Planning and Programming." ***Corrections Today 53*** (July 1991).

Matthews, Don Q. "The Design of the Management Information System." New York, 1971.

Margolis, Philip E. "The Random House Personal Computer Dictionary." Random House, 1991.

McKeen, David R. "Sounding the Alarm. Making the Most of Your Metal Detector." ***Corrections Today 52*** (July 1990).

National Fire Protection Association. "Fire Safety in Correctional Facilities: Instructor's Manual." Washington, D.C.: U.S. Department of Justice, National Institute of Corrections, NFPA No. SPP 69A, 1981.

North American InTeleCom, Inc., San Antonio, Texas.

O'Connor, Vincent. "Alaskan Canine Units Keep Inmates on a Tight Leash." ***Corrections Today 52*** (July 1990).

Parker, Sybil P. "Electronics and Computers." 2nd edition. New York, 1987.

Perimeter Products, Mountain View, California.

PGT-Outokumpu Electronics, Bethesda, Maryland.

Protective Technologies International, Inc., Salt Lake City, Utah.

Roper, C. A., and Bill Phillips. "The Complete Book of Locks and Locksmithing." 3rd edition. TAB Books, Blue Ridge Summit, Pennsylvania, 1991.

Schwarzmann, Stephen T. "Retaining Dignity. High-Tech Metal Detectors Offer Body Search Options." ***Corrections Today 52*** (July 1990).

Sentry Products, Inc., Santa Clara, California.

Sheridan, Francis J. "High-Tech Perimeter Security Foils Escapes." ***Corrections Today 52*** (July 1990).

Simplex Time Recorder Co., Gardner, Massachusetts.

Smith, Alpheus W., and John N. Cooper. "Elements of Physics." New York, 1979.

State of Hawaii. "National Survey of Corrections Information Systems." Honolulu: Department of Corrections, October 1989.

Stearne, Ivan G. "How to Design/Build Remote Control Devices." TAB Books, Blue Ridge Summit, Pennsylvania, 1981.

Stentofon Communications, Inc., Kansas City, Missouri.

Sound Powered Communications, Trenton, New Jersey.

Southern Steel Company, San Antonio, Texas.

"Technology and the Direct Supervision Jail." ***American Jails*** 3 (Winter 1990).

Telecourier, Inc., Naples, New York.

USER FEEDBACK FORM

Please complete and mail this self-addressed, postage-paid form to assist the National Institute of Corrections in assessing the value and utility of its publications.

1. What is your general reaction to this document?

___ Excellent ___ Good ___ Average ___ Poor ___ Useless

2. To what extent do you see the document as being useful in terms of:

	Very Useful	Of Some Use	Not Useful
Providing new or important information			
Developing or implementing new programs			
Modifying existing programs			
Administering ongoing programs			
Providing appropriate liaisons			

3. Do you feel that more should be done in this subject area? If so, please specify what types of assistance are needed.

4. In what ways could the document be improved?

5. How did this document come to your attention?

6. How are you planning to use the information contained in the document?

7. Please check one item that best describes your affiliation with corrections or criminal justice. If a governmental program, please also indicate level of government.

___ Dept. of corrections or prison
___ Jail
___ Probation
___ Parole
___ Community corrections
___ Court
___ Juvenile justice
___ Police
___ Legislative body
___ Professional organization
___ College/university
___ Citizen group
___ Other government agency
___ Other (please specify)___________________

___ Federal ___ State ___ County ___ Local ___ Regional

8. **OPTIONAL:**

Name______________________________ Agency ______________________________

Address____
____

Telephone No. (____________)_____

Please fold and tape closed.

BUSINESS REPLY MAIL
FIRST-CLASS MAIL PERMIT NO. 14045 WASHINGTON, DC

POSTAGE WILL BE PAID BY NATIONAL INSTITUTE OF CORRECTIONS

All-N: PUBLICATIONS FEEDBACK
NATIONAL INSTITUTE OF CORRECTIONS
320 FIRST ST NW
WASHINGTON DC 20277-4045

National Institute of Corrections
Advisory Board