

U.S. Department of Justice
National Institute of Corrections



The Security Audit Program

A How To Guide and Model Instrument
for Adaptation to Local Standards, Policies, and Procedures

020294

Introduction: Security Audits

A *security audit* is a process for determining the extent to which policy, procedure, standards, and practice combine to provide a safe and secure institutional environment. Included in this process is a detailed evaluation of every major aspect of an institution's security program.

The work of the security audit may be best described as *risk assessment*. The function of risk assessment is to determine the likelihood of a significant security problem or vulnerability to injury, escape, disruption, or destruction of property due to inadequacy of policy, procedure, physical plant and/or performance. Risk assessment, hence a security audit, is the process of determining the risk remaining after all the normal management safeguards have been applied, including clarity of policy, procedure, and post orders, training, physical plant accommodation and daily supervisory activities.

Moreover, a quality security audit program allows for all of the detailed assessment described above, but does so in a non-adversarial manner providing for a "win-win" opportunity for everyone involved. This includes agency and institution management, supervisors at all levels and line staff.

By avoiding an "I gotcha" philosophy in favor of a cooperative look at how we can strengthen and enhance an institution's security posture, the detrimental impact of unhealthy competition and divisiveness can be eliminated. Staff at all levels working together is the most effective way to bring to life an overall "security mind set" within the facility!

Protection of the public, staff, and inmates is the primary mission of any prison system. Experience has proven that the development and implementation of a comprehensive security audit program is a major step in reducing the risks that are endemic in prison operation. This document can be helpful in achieving that end.

Table of Contents

	Page	
Chapter I		
The Development of a Security Audit Program	1	
Chapter II		
How to Perform a Security Audit	12	
Chapter III		
The Audit Report	22	
Attachment 1		
Narrative Security Audit Format (sample)	28	
Attachment 2		
Tabular Security Audit Format (sample)	32	
Attachment 3		
Department of Corrections Security Legislative Report	33	
Chapter IV		
How to Use the Security Audit Instrument	36	
Audit Instrument:		
Section 01	Armory/Arsenal	39
Section 02	Communications	44
Section 03	Inmate Counts	47
Section 04	Control Center(s)	50
Section 05	Controlled Movements	54
Section 06	Use of Force	56
Section 07	Hazardous Materials Management	60
Section 08	Inmate Mail	63
Section 09	Inmate Visiting	65
Section 10	Inmate Property	69
Section 11	Inmate Work Assignments	72
Section 12	Inmate Transportation	76
Section 13	Key Control	81
Section 14	Perimeter Security	91
Section 15	Physical Plant	100
Section 16	Post Orders	104
Section 17	Searches	106
Section 18	Security Inspections	113
Section 19	Segregation (Special Management)	116
Section 20	Tool and Sensitive Item Control	122
Section 21	Emergency Plan	131

Chapter I

The Development of a Security Audit Program

The past twenty years have been characterized by rapid growth in prison construction and an accelerated evolution in prison and jail design. Perimeter barriers, locking systems, video and communication technology, and alert systems have been vastly improved. These improvements have resulted in more efficient, effective operations and enhanced safety of staff, inmates, and the community. Good sight lines, integrated with sound security hardware and reliable technology have become the hallmarks of efficient, safe, secure, and humane correctional housing. Such enhancements balance cost effectiveness, ease of maintenance, and efficient use of staff resources. Without question, modern prison designs represent significant improvement over many of the models that preceded them.

As important as these improvements are, however, they cannot of themselves provide a safe, secure, and humane environment. They are only a part of what is necessary to ensure a sound security plan, program, and operation. The most innovative design and advanced technology cannot substitute for well-trained staff and good security practices that are based in comprehensive security policies, procedures, regulations, and rules that are clearly written, standardized, and fully implemented. Even then, without a well-planned, comprehensive monitoring program, effective security practices cannot be sustained over the long term.

■ The Security Audit Program

A nationwide review of after-action reports of escapes, staff assaults, hostage situations, disturbances, and other serious problems reveals few instances in which malfunctioning locks or electronic detection systems, insufficient razor wire, or other deficiencies in physical plant or technology were responsible. Rather, most serious security breaches occurred because one or more staff members took a "shortcut," did not know what was expected of them, or simply failed to follow established security procedures. Though weaknesses in the physical plant may have contributed to the problem, it was usually the failure of staff to attend to business that was at the heart of the incident. In other words, "people-system failures," not "physical-system failures" account for most security breakdowns.

This unfortunate reality points to the need to establish a comprehensive monitoring program. An adage that is familiar in security

You get what you *inspect*, not what you *expect*.

circles, "you get what you *inspect*, not what you *expect*," or stated another way, "Staff will *respect* what you *inspect*" is certainly true; underscoring the fact that what the "boss" pays attention to will be viewed as important by subordinate staff. It is through consistent monitoring that the agency leaders and institution administrators/managers affirm the critical importance of standards, policies, procedures, and sound security practice.

No longer can institutions be operated as separate and autonomous "kingdoms" in which sound, commonly held security principles are ignored. Increasing public sensitivity to correctional issues, rampant litigation against corrections officials, increasing size and complexity of facilities, existing and emerging national standards, and a growing knowledge base of professional practice requires that correctional systems and their individual institutions operate within established and broadly-held security standards. It is through a program of security monitoring/auditing that an agency ensures that such practices continue in place, without compromise.

Definition

"Security audit" is a process for determining the extent to which policy, procedure, standards, and practice combine to provide a safe and secure institutional environment.

Types of Audits

There are three types of audits in correctional facilities through which aspects of security operations are monitored. The first, an audit of standards, is based upon American Correctional Association accreditation standards or is a self-audit based on similar standards adopted by an agency or association of agencies. A standards audit is a well-accepted and valid way of assessing the overall operation of a correctional facility. However, it lacks the comprehensiveness, intensity, and security focus that are necessary to identify numerous elements of risk to which many security operations are vulnerable.

The second type of audit, the policy audit, is an effort that seeks to ascertain whether or not centrally mandated policies and related procedures are in place. Such audits are valid in determining institutional

compliance with agency policy but generally fall short of identifying weaknesses in the operation caused by deficiencies in training, supervision, and/or practice that may create risk. A policy audit of key control, for example, may determine that policies and procedures are in place but this type of audit will not often determine if, in fact, they are being carried out in practice or that essential procedures beyond those mandated in agency policy are appropriate. For example, a policy audit may find an institution to be in compliance with policy requiring the Warden to authorize the assignment of permanent (take home) keys. But, such a finding does not speak to *which* keys are taken home by *whom* and there may be literally hundreds of such sets assigned that are not routinely inventoried. Such a condition may suggest a key control system that is out of control while having in place each required policy.

The third, the security audit, focuses on security operations. Although standards and policy are important aspects of such audits, the primary focus is the security systems and their operational implementation on a daily basis. This audit is a "where the rubber meets the road" experience that, when properly conducted by persons who are intimately familiar with security principles, identifies weaknesses in the program that create risk to safety and security. Although standards and policy audits are important, the security audit is essential in identifying "slippage or cracks" where policy and procedure enhancements are necessary. Such subtle changes over time as new staff entering the institution workforce; experienced staff becoming complacent; weakened supervision as new, inexperienced supervisors are promoted; aging physical plant and equipment; addition of new buildings and equipment; expanded use of inmate workers; etc. can render policies and procedures

dangerously deficient and ineffective. Security auditing is a “real time” process.

Outcome

The *outcome* of the security audit may be best described as a “**risk assessment**” which may be defined in this context as “a determination of the likelihood of significant safety or security problems or vulnerabilities to injury, escape, disruption or destruction of property due to inadequacy of policy, procedure, and/or staff performance.” Risk assessment is the process of determining the risk remaining *after* all the normal management and operational safeguards have been applied, including clarity of all instructional documents, training, and daily supervisory activities. Factors creating such risks may include poorly designed policy; inadequate procedures; overlooked standards; a facility design inappropriate to a changed inmate profile; inadequate training; or inattention of staff to the requirements of their position.

This is accomplished through intensive observation, discussion with staff, and the testing of internal controls. In a security audit program, auditors are addressing five basic questions that, when objectively applied, provide an assessment of risk and vulnerability with recommendations for rapid correction of the condition of risk. These questions are:

- What is the current condition? (a snapshot of reality)
- What should it be? (standard, policy, criteria, etc.)
- Why is it important? (probable effect or impact of the current condition)
- How did this condition come about? (cause)

- What will correct the problem? (recommendation)

As these questions are systematically addressed, the adequacy of policy and procedure is determined, staff practice as related to expectations is observed, staff knowledge of job requirements is examined, and equipment and hardware are inspected. With periodic security audits, the entire institution operation is likely to be strengthened.

Reasons for a Security Audit System

Why should a correctional agency have a comprehensive security audit program? The benefits to the agency, institution, and community are many. We will discuss several here.

It is through monitoring that assurance of compliance can be gained and then only over time as the operation becomes self-monitoring in anticipation of monitoring by the leadership in the organization.

1) *Weaknesses, deficiencies, and areas of vulnerability in the institution operation will be identified.*

Without a comprehensive and systematic review of facilities, operations, and equipment, it is unlikely that weaknesses and deficiencies will be reliably identified before becoming problematic. Inability to “see the forest for the trees” inhibits our ability to identify weakness, deficiency, and vulnerability without specific mechanisms that force attention to that level. Staff familiarity with their surroundings is both a “blessing” and a “curse”: A blessing as it contributes to efficiency of performance but a curse as it contributes to complacency and development of “short-cuts” that create risk.

2) *Compliance with agency and institution endorsed standards, policies, and procedures is assessed.*

It is only through targeted review and observation of policies, procedures, practices, and outcomes that leadership can be assured

that expectations are being met. Without an audit program, deficiencies in the security operation are often discovered only as inmates test the system through assaults, escapes, or other undesirable activities. It is through monitoring that assurance of compliance can be gained and then only over time as the operation becomes self-monitoring in anticipation of monitoring by the leadership in the organization.

3) *Equipment, locking mechanisms, tool and key systems, etc., that are inoperable, inappropriate or inadequate are identified.*

During NIC's *Conducting Security Audits and Emergency Preparedness Assessment* seminars, in which participants are trained through actual participation in audits and assessments, serious problems are frequently identified. Emergency keys that no longer fit locks because of wear to the lock or changing of the lock, air pack breathing devices that are inoperable, policies and post orders that are inaccurate and ineffective because of facility modifications, perimeter intrusion systems that are shut down or inoperable, tool control systems which do not fully account for tools, are but a few of the serious issues that have been frequently identified. Without monitoring systems, the likelihood of such security breakdowns being undetected is high in most facilities.

4) *The efficient and effective application of security resources is reviewed.*

It is not uncommon that temporary posts/assignments become permanent, critical but unpopular activities are abandoned, security standards or policies are compromised, or other "slippage" occurs simply due to the press of every day supervisory requirements or staff

Managers who assume that, it is in fact done because it is written in policy, reinforced in procedures and post orders, clearly articulated and expected will invariably be disappointed.

inattention. Many such costly "loose ends" to the institution, both in manpower and safety/security, will be identified through the auditing of security operations.

5) *"Best practices" are identified and are shared throughout the agency.*

Even as staff have the capacity to become complacent in performance, they have the capacity to refine their activities to a point of vast improvement over the stated procedure or expectation. It is important that such initiatives be identified, recognized and the improvements shared with other parts of the organization. Failure to identify and reward initiative will most often discourage further initiative. Such recognition provides for and reinforces the positive role of the audit process to the staff subject to its scrutiny.

Essentials of the Security Audit Program

Security audits that "just happen" and are not part of an authorized, planned program designed to upgrade security operations, are almost invariably met with resistance. There is often a perception by institution managers of having been singled out and findings are often disputed and resented. There are several essentials that form a foundation for an agency security audit program that will be viewed as legitimate and helpful.

Administrative Support

The first essential step in developing an audit program is the marshaling of the full support and participation of top administrators (Central Office and Institution leaders) in planning and preparing for security audits. This support will make a critical difference in the response of institution staff to the audit process. The following are some ways by which administrators

convey an audit intent that is helpful and non-threatening:

- Facility leadership clearly states their commitment to the audit program and their intent that it be a helpful tool to their staff;
- Audit objectives are clearly articulated in terms that emphasize safety and security and a focus on “what,” not “who.” It is acknowledged that deficiencies will be identified but that staff will not be targeted;
- Behavioral and performance expectations for auditors are clearly articulated and care is exercised in selecting auditors who are knowledgeable and creditable;
- Audit team members are thoroughly trained *before audit activities begin*;
- Security standards against which institutional practices may be measured are reviewed, clearly articulated, and reinforced;
- There is commitment to a “fresh eyes approach” in which there is willingness to take a new look at any and all policies, standards, and practices;
- Audit objectives include identification and communication of “best practices” as well as areas of vulnerability. The recognition of staff who are demonstrating sound security practices and awareness is encouraged at verbal debriefings and in written reports;
- Leadership encourages the “celebration” of good safety and security findings and outcomes, fosters a learning environment in which the audit is a learning strategy, and prohibits condemnation of staff when weaknesses or deficiencies are identified.

In an atmosphere in which positive findings and results are met with celebration and deficiencies are met with strengthened policies, standards, and practices, updated training, and enhanced supervision; staff will grow to accept and support the audit process.

Their acceptance will be in a spirit not unlike that of acceptance of an annual physical examination: perhaps inconvenient, but essential to their long-term betterment.

Security Audit Policy

The second essential is the establishment of the authority and a mandate for security audits. At minimum, the policy should address the nature of the program, including frequency of audits, whether announced or unannounced, criteria for selection of auditors, training requirements for auditors, type of audit report required, and the expectations of the agency regarding the institution response to the report. The security standards and security audit instrument that are authorized for application should be referenced by location and most recent date of revision.

The Policy should address the type of audits that are required. In some jurisdictions, a combination of *internal* audits and *external* audits are authorized and mandated. Internal audits, those conducted by staff within an institution, are sometimes mandated between external audits, audits conducted by a team or staff from outside the institution. In other jurisdictions, internal audits are *pre-audits* and are conducted by institution staff just prior to the external, agency audit.

Internal audits are not recommended as the sole audit activity. It is often found that auditors find it difficult to objectively point out shortcomings by friends, fellow-workers, and supervisors. For that reason they lack credibility. In addition, the “forest for the trees” condition exists and they may not identify risk or vulnerability as they audit conditions in which they work every day.

Conversely, external audits tend to be more objective and thorough. They may be announced or unannounced. An advantage of unannounced audits is that the institution is

viewed in an operational condition more closely approximating "normal". An advantage of announced audits is that the institution has an opportunity to prepare and correct conditions that they know to be deficient before the audit occurs. Some jurisdictions have found a combination of announced and unannounced audits to be effective: a schedule of unannounced audits sometimes being established on a random basis.

A third approach to auditing is contracting with experts from outside the system or institutions. This has the advantage of bringing expertise from a broader experience base and will normally be free of allegiances that get in the way of objectivity. Disadvantages of this approach include cost, lack of knowledge by outsiders of labor agreements, statutes, administrative philosophy, and the history and various nuances that make the agency what it is. Most jurisdictions contract with outside experts in exceptional circumstances when credibility and objectivity are essential and cannot or will not be perceived to be so in an agency-based audit.

Security Operations Standards

Essential in the development of a security audit program is the development of a manual of security operations standards against which various components of the security operation can be measured. Without it, the auditors are "shooting at moving targets" as varying interpretations, understandings, and/or perceptions of the agency standard get in the way of assessments of practice. The development of an agency-wide security audit program provides opportunity and rationale for the establishment of such standards for review and buy-in by institution managers. The security audit standards of an agency and its institutions constitute the "bill of particulars" by which the agency/institutions operate. The

standards reflect the minimum level of acceptability for each component of security operations and, as such, are the gauge by which the security audit program measures.

Security standards should be based in the mission of the agency/institution and incorporate:

- Agency/institution policy, post orders, procedures, etc;
- ACA security standards, as applicable;
- Best security practices as identified in discussion with security professionals and agency/institution experience.

Security standards should be adapted for application to various security/custody levels and subject to the review and the input of all security managers and facility managers who will be required to comply with these standards.

Security Audit Instrument

Finally, a Security Audit Instrument must be developed that is consistent with the security operations standards of the agency and guides the auditors as they conduct the audit. Consistent use of an instrument endorsed by the agency will go far in reducing charges by managers that are being "targeted" or that their audit was unfair.

There are numerous examples of audit instruments available for review by contacting other state security managers. These instruments can be helpful in reviewing/developing security standards and an audit instrument as can the document, *Guidelines for the Development of a Security Program*, available from ACA. Perhaps the most comprehensive institution security document in print, this document can serve as a working manual in developing an instrument. However, whatever tool or other-state example is used, like the instrument included in this document, the tool or example must be customized to the agencies' mission, policy and procedures, and security standards to be effective. "Ownership" and

'buy-in" by everyone involved is critical to a successful program.

It is important to recognize that because of differences in standards from jurisdiction to jurisdiction that a universal comprehensive security audit instrument does not exist and, arguably, cannot be developed.

Security audit instruments may be in various formats. Generally, however, they fall into two basic types, the narrative instrument and the tabular instrument.

Narrative Instrument:

The narrative instrument is a listing of points of review that represent the priority concerns of an agency as related to basic security topical areas (searches, visitation, key control, etc.). Following each point of review, there is generally space for the auditor to record an observation or comment (*see Attachment #1*).

For ease of use, this format is unsurpassed. However, it requires that the auditors be experienced security professionals because the points of review usually consist only of the priority concerns in the topical area and do not attempt to list all of the concerns. This format assumes that the auditor will observe other security-common sense matters and issues related to the listed points of review.

In addition, this format lends itself well in situations where auditors from outside the system, who are not familiar with in-agency, security-specific policy, procedure, or practice, conduct the audit. It may also be preferred in an agency in which security standards have not been clearly articulated.

This audit format is less likely to produce a checklist type outcome in which auditors are focused on the format. Its use encourages and allows for constructive thinking and broader exploration of issues

than does use of a tabular or checklist-type format.

A negative aspect of this format is that points of review may often lack reference to an established set of standards for security practices; however, this is by choice rather than necessity. In development of the instrument, each point of review can be identified in its relationship to Security Operations Standards or, as in the tabular format; it can be assumed that all points of review are agency policy, if the agency so chooses.

Some may argue that this format does not generate a complete record of the security operation at the time of the audit—as may a tabular (checklist) format. Caution would suggest that *no* instrument generates such a complete record. The skill and knowledge of the auditors—not the instrument—determine the completeness of the assessment of the security operation at a given point in time. Finally, its conversion to an action plan may be more cumbersome and the product likely to be more narrative in nature than a tabular format, but it is likely to be more informative about the issue being addressed.

Tabular Instrument:

The tabular instrument is arranged in a table format that provides information and space for recording information (*see Attachment #2*). Similar to the narrative instrument, the information is organized according to basic security topics (searches, visitation, key control, etc.).

Normally each row in the table addresses a specific standard. It is common for one instrument to contain several hundred standards. The standards should be officially accepted by the jurisdiction and are referenced in security policy. This feature ties the instrument and audit activity to the larger

system of agency activity related to security program operation. The information in the instrument may only be a statement of the security standard: others include a citation of the specific agency policy that describes the standard. For the sake of efficiency, other instruments are constructed with the assumption that all standards described are correct expressions and interpretations of agency policy.

Each row contains space for recording information related to each standard, including a checklist and a space for auditor comment. These spaces are intended to allow the auditor to record their observations and conclusions with respect to each standard. Some of the options they may be considered for the check listings are as follows:

- *Check "C" for Compliant:* This designation means that the practice observed in terms of systems operation and staff performance is compliant with the standard.
- *Check "NC" for Non-Compliant* This designation means that the practice observed in terms of systems operation and staff performance is not compliant with the standard.
- *Check "EC" for Essentially Compliant:* This designation means that the practice observed in terms of systems operation and staff performance is nearly compliant with a few adjustments to be made in order to achieve compliance. This designation should never be given without some direction provided in the comments section that *describes the adjustments to be made in order to achieve compliance*
- *Check "E" for Exception:* Occasionally a standard may not apply to a facility being audited. An example may be standards related to non-contact visitation may have no application to minimum or community custody facilities. As with the EC designation, this designation should never

be given without some explanation from the auditor.

A comment section is also provided to allow the auditor to record observations related to the nature of deficiencies and information for improving security practices.

There are several advantages to the tabular instrument:

- It allows for the collection and coordination of a large amount of security information.
- It can be quite complete covering most or all of the security performance standards of the agency.
- Given it is produced through a database or table management software, the information can be converted into different kinds of reports using the same base of information. Some examples are converting the original audit report into such things as a simplified action plan for facility response, or an executive summary focusing on non-compliant issues, compliant, and exemplary practices. The conversion may easily reduce a thirty to forty page document to a very brief action plan of just a few pages.
- It has the potential to relate policy to standards, and standards to sound conclusions based upon observed practices.

The disadvantages of the tabular instrument include:

- It can be so extensive and detailed that it is a constant temptation for the auditor to be absorbed in its use and spend less time observing the quality of security practices. As a result, the audit takes on the character of a "paper audit" rather than one more concerned with actual staff performance.
- Complicated versions become very staff intensive, absorbing critical resources in trying to produce and understand reports.

- Should the instrument be “scored,” it may cause the organization to be more concerned with point totals than security practices.

The choice of the agency in terms of the format and content of the audit report should fit the needs and resources of the agency, and should be user friendly to the people it serves. The design of the instrument is important for the reasons discussed above. However, it is more important that the agency initiate and promote a professional audit program and not be delayed or hindered by difficulties related to format and content.

Most instruments include some or all of the following:

- Audit information page(s) with space for the name of the facility being audited, date of audit, and names of the auditors;
- Instructions for use of the instrument as a self-audit tool (optional);
- Table of contents listing the security categories contained in the instrument;
- Points to be reviewed (security standards and expectations) by category;
- Columns for indicating compliance/non compliance, yes/no, or other indicator of auditor's finding;
- Space for additional categories as may be needed (for example: a specialized program facility may have special security needs); and
- Space for auditor comments.

The audit instrument, whatever its design may include some, if not all, of the following categories:

- Armory/Arsenal
- Communications
- Contraband/Evidence Management
- Inmate Counts
- Control Center Operations
- Controlled Movement
- Fire Safety
- Food Service

- Hazardous Materials Management
- Health Services
- Inmate Mail
- Inmate Housing
- Inmate Visiting
- Safety and Sanitation
- Searches
- Segregation & Special Housing
- Tool Control
- Inmate Work Assignments
- Inmate Transportation
- Key Control
- Perimeter Security
- Physical Plant
- Post Orders
- Release & Discharge
- Emergency Plan

The development of written security operations standards and an audit instrument can be an exhausting task. As in many other circumstances, there may be no need to “reinvent the wheel.” Many agencies have developed such standards and an instrument, which may be readily adapted to another agencies’ use. This document contains an audit instrument designed for that purpose.

Carefully developed policy, standards, and instrument are the underpinnings of a sound security audit program. They provide the authority, intent, direction, units of measure, and measurement tool. Without them the audit can be less than credible, lacking in official sanction, and random (as opposed to planned, methodical, and comprehensive), both in terms of process and outcomes.

In summary, there are few activities that are more important than the monitoring of the security practices upon which the health, safety, and security of staff, inmates, and the community depend.

It is through monitoring that risk and vulnerability is identified. It is through

- Provide initial training in knowledge and understanding of the audit instrument, its application;
- Provide initial training, post-audit debriefing, and annual update on audit technique and protocol: the *how to's* and the *should not's*.
- Accredit the training course so that staff may receive credit for participation.

A key element of auditor training, technique will be discussed in the following chapter. It cannot be over-emphasized that the validity and effectiveness of a security audit will be in direct proportion to the knowledge and skill of the auditors.

Chapter II

How to Perform a Security Audit

As we have indicated, a primary function of a security audit is to identify areas of vulnerability and thereby enhance the safety and security of staff. Done well, however, the audit has other very significant benefits. The greatest of these is a forum for teaching sound security practice and for learning from the work and experience of others. This being the case, the audit should be viewed as a welcome and helpful process. Unfortunately, institution staff most often perceive an audit to be a negative experience.

In most instances, the reason for this perception is that audits have been historically conducted in a confrontational manner (or are viewed as confrontational) and tend to mobilize the defensiveness of those whose area of responsibility is being audited. In the experience of many staff, audit findings that are “negative” have resulted in embarrassment, caustic reprimand, and even discipline. When the security audit is perceived to be an “I gotcha” exercise, an effort to catch staff doing wrong, rather than a tool to enhance safety and security, staff will invariably react defensively. This can be a difficult perception to overcome. It is critically important that steps be taken to develop a security audit program that conveys a non-confrontational, helpful perspective.

Once weaknesses or deficiencies are identified, the institution manager should be required to develop a plan to address the problems identified. Training, modified post orders, new equipment, changed procedures,

or a host of other remedies can be developed. *Discipline of staff should NOT be one of them.* Auditing is for the purpose of learning and improvement: supervision is for the monitoring and correcting of staff. If discipline becomes necessary, it should grow out of the supervisory relationship.

When the security audit program is perceived by staff to be an “I gotcha” exercise, rather than a tool to enhance safety and security, staff will invariably react defensively.

A second reason for security audits being viewed as negative or meaningless is the failure to use credible auditors. As indicated in Selection of Auditors in Chapter 1, credibility of auditors is critical to the success of the audit program. When staff view auditors with a “what do *they* know about it” attitude, findings may be ignored.

Staff should be reminded of the seriousness of their responsibilities. Complacency and routine is the enemy of sound correctional practice. Deficiencies *must* be identified and corrected: risk and vulnerability *must* be recognized and diminished. Staff should be reminded that the safety and security of the working/living environment is everyone’s responsibility and in everyone’s best interest.

Understanding the Security Audit

The security audit process is not just a “paper process” composed of checklists. It is a process requiring the auditor’s full attention and application of all her/his skills. It requires understanding of the correctional imperatives and the correctional environment. The auditor must be objective, experienced, open-minded, flexible, willing to listen, and alert to the positives and best practices observed, as well as pointing out deficiencies.

A correctional institution is a complex environment in which there is an ebb and flow of control and privilege, which is largely monitored in the relationship of the keeper and the kept. Much of what “goes wrong” in the security operation develops in that complex relationship. The audit process must be of a nature to understand the “ebb and flow” of the subject institution and delve into what is really occurring on a day-to-day basis in the interactions between staff, inmates, and others.

Between institutions, correctional practice and processes will vary based on differences in mission, staffing, offender population, security and custody level of the institution, types of programs offered, and the physical plant. These differences require variance in security operations from one institution to another, while agency security *standards* prevail in both. As auditors move from one institution to another, they must have the understanding and capacity to incorporate the variances into their thinking as they assess the operation

A *fresh eyes* approach is an absolute necessity in conducting a comprehensive audit. Staff often become complacent with established routines and mundane tasks. “Short-cuts” abound and some new staff may have never been taught proper procedure. Supervisors are not immune to such complacency and they, too, can “walk past” and not notice breaches or violations in security. *Fresh eyes* specifically focused on security and a new perspective will identify many issues and situations where staff have created shortcuts, abandoned essential security practices, or simply become complacent in the routine of the day. Auditors

should not shrink from the responsibility of identifying risk or vulnerability that may exist, irrespective of the reasons for its existence.

Preparation for the Audit

The seriousness of the auditing responsibility should be reflected in the preparation.

The auditor must be well grounded in the agency’s Security Operations Standards. These, of course, are the basis of the audit and all operations must be assessed in the light of

A correctional institution is a complex environment in which there is an ebb and flow of control and privilege, which is largely monitored in the relationship of the keeper and the kept. Much of what “goes wrong” in the security operation develops in that complex relationship.

these standards. If there is lack of clarity or contradiction in standards, it is essential that these be addressed, in writing, so that all auditors and institution managers share the same

understanding. For example, a standard that says “periodic security checks must be made” will be interpreted in many ways—15, 30, 45 minutes—and is not a measurable standard. It will be helpful to define “periodic” if disputes of interpretation are to be avoided.

The auditor must also be very familiar with the Security Audit Instrument: so familiar, in fact, that here is little reliance upon the document during the audit. It cannot contain all the points of review relevant to every institution and every situation. The Instrument should serve to identify critical points of review, but there will be many issues observed that are not mentioned in the audit instrument, each issue leading to another until the point and scope of risk or vulnerability is exposed. The security experience and knowledge of the auditor will provide the insights and understandings that will guide him/her in a productive direction as questionable issues are observed. Lack of

familiarity with the instrument and sound security practice will cause the auditor to be “tied” to the instrument and the result is likely to be a “paper audit” outcome.

The security experience and knowledge of the auditor will provide the insights and understanding that will guide him/her in a productive direction as questionable issues are observed.

It is recommended that each institution be required to prepare a packet for auditors that contain, at minimum, the following information.

- Institution Mission
- Organizational Chart with names through First-line Supervisors
- Current foot-print of the institution
- Program description
- Inmate profile
- Special issues or problems of which auditors should be aware or to which the Warden would like them to give attention.

This information will enable the auditor to achieve a greater level of comfort as the audit begins.

■ Security Audit Technique and Protocol

Audit Technique

As with most activities, adopting a technique or method makes the task easier. And though security auditing is not an exact science, there is technique involved that makes a complex task less complex and ensures that the audit will be comprehensive. The training of auditors should include extensive discussion of audit technique and protocol.

It has been said that a comprehensive assessment/audit must include four elements:

- 1) What is written? **READ**
- 2) What is said? **LISTEN**
- 3) What is done? **QUESTION**

4) What is done? **OBSERVE**

This is the heart of auditing technique. All four elements are important in achieving a valid outcome. They provide checks and balances and enable the auditor to get as near to actual practice as is possible, given limitations of time and the magnitude of the task.

READ:

- Are policies and procedures complete, up-to-date, and accessible to those who need to know?
- Are policies, procedure, and post orders clearly written and in user-friendly format?
- Do post orders and policies conflict? If staff are aware of the conflict, a situation of stress/tension exists and performance will suffer.
- Do posted notes, memos, and orders at officer stations and elsewhere countermand policy, procedures, or post orders? Is the writer a duly appointed authority?
- Are logs, form, inventories, etc., legible, complete, current, and in compliance with requirements as stated in policy, procedure, or post order? (Review both current and historical logs, inventories, reports, etc.)

LISTEN:

- Actively listen to staff—not only in response to your questions but to what they want to tell you. Inmates may wish to discuss issues as well. These discussions can provide an auditor with insight into the tone and climate of the facility.
- Hear staff comments about “audits”: it will help you understand their perspectives and attitudes and in forming your approach as you do your work.
- Listen to what staff are *not* telling you. They may be reluctant to tell you outright that they rarely see a supervisor or

administrator at their post but you can “hear” that message in other ways.

- Hear words, tone, and expressions that suggest fear, anger, pride, complacency, and boredom.

Question:

- What is the facility/staff experience with audits? How do they perceive audits...a “gotcha” exercise? Are they likely to be helpful or to hide what they can? Awareness of staff attitudes can be helpful to the audit team in knowing how to approach the audit.
- Do staff have recommendations for enhancement or improvement of a specific aspect of operations? They will sometimes share ideas without being asked but by asking, the auditor can involve them and elicit information about concerns they may have about their post. Suggestions by staff should be noted as a positive contribution (with the staff member’s name) during the debriefing session and in the final written report. Doing so will help build staff confidence and trust in the audit process.
- Conduct verbal on-post testing. For example: Does the staff member understand his/her responsibility and/or proper response to a specific type of emergency? This is sometimes referred to as the “what if” exercise.
- Conduct on-post proficiency tests. Does the staff member know how to safely operate a specific piece of equipment?
- Does the staff member understand the post orders for the specific area of responsibility?

OBSERVE:

- Don’t rely only on written policy/documentation; review practice. The written word tells only a fraction of the story in security assessments. Does practice conform to policy, procedures,

and post orders? *Are we doing what we say we are?*

- Coordinate observation during formal counts or other institution activity. Separate the team to observe various aspects of the count or other activity.
- Observe operations. Note the degree to which practice conforms to policy requirements, post orders, etc. Observe staff searching a vehicle, inmate skin and frisk searches, visitor access to the facility, and the use of metal detectors and other technology.
- Test security systems. For example, test the key control system by having a staff member take you from outside to a specific point inside the facility, perhaps using emergency keys. Inform staff that you are conducting the test, state the purpose of test, and explain that the tests are meant to be learning opportunities.
- Complete at least one systems check during the audit.

Assessing the Environment

Though points to be reviewed are defined in the audit instrument and suggested in standards, policy, procedure and post orders, the institution environment should also be assessed. The institution environment in which staff work and inmates live is important. If it is positive and healthful, it promotes growth and actualization: if it is negative, it will be demoralizing and destructive. Although there are few “hard” issues to audit, there are many indicators that can be observed that will give an auditor a sense of the environment.

Once again, solid security experience comes into play: with experience comes an ability to “feel” or “read” the prison environment and to identify aspects of the facility and operation that are suggestive of negativity. Among the aspects of the facility

and operation that the auditor must review are the following:

- *Sanitation:* Are good sanitation practices enforced *throughout* the facility? A lack of acceptable sanitation can frequently indicate serious management and supervision issues within a facility. Do sanitation practices create an environment conducive to inmate pride and positive staff morale, while providing opportunities for inmate jobs? Are there waste, clutter, facility deterioration, and unclean conditions that may create a fire, health, safety, or security hazard?
- *Facility Tone and Climate:* What is the inmate's frame of mind? What type of complaints do they have? Is the general feeling within the facility positive with inmates making eye contact with staff? What is the nature, frequency, and tone of grievances? Are grievances taken seriously? Are staff comfortable and confident in confronting and correcting inmates in order to enforce institutional rules and other requirements?
- *Staff Morale:* Are staff positive and up beat? Do they take pride in their work? Are they generally cooperative with auditors or reluctant to speak up? In the later situation, auditors should consider the reason for reluctance and lack of cooperation: it may be because of punitive supervision or leadership or generally low morale. If it is a pervasive attitude, it should be noted in the audit report. Remember, when staff morale is low, staff are not in tune with the institution mission and security will suffer and complacency will become commonplace.

■ The Auditor's Role

The "Good Neighbor" Auditor:

Auditors sometimes have difficulty understanding their role and the limits of their responsibility. Put in a position to observe, question, and report deficient practices, there is often a temptation to feel a sense of "power" in the position. In a correctly designed audit program, there is NO position power in the auditor role.

The role of the auditor is to *identify* and *report* (to designated leaders) conditions, which in his/her opinion are in variance with agency policy and standards and, in most agencies, *recommend a more appropriate condition. All decisions concerning the report and recommendations are then in the hands of decision-makers.*

As the role is properly understood, auditors come to be viewed by staff as vehicles for communicating ideas, needs, and workplace

Proper understanding of his/her role provides the auditor freedom to identify areas in which improvements could/should be made without being limited by factors impinging upon the situation: cost, staffing, labor agreements, facility limitations, etc.

frustrations to the leadership of the organization. These ideas should be passed on, perhaps as part of a recommendation, and the staff given credit by name for the idea or practice. Proper understanding also provides the auditor freedom to identify areas in which improvements could/should be made without having to consider all of the factors impinging upon that situation e.g. cost, staffing, labor agreements, facility limitation, etc. In so doing, s/he "pushes the envelope" and encourages consideration of options that may have previously been ignored or denied because of the known limitations. If the situation/condition poses potential risk or vulnerability, it should be reported irrespective of such factors. The decision-

makers then have responsibility to determine what is to be done, if anything, to correct the deficiency.

Auditor-Staff Relationships:

When entering an area, audit team members must *always* be introduced to staff and the purpose of their presence in the facility explained. Remind staff that the purpose of the audit is to review operations and identify ways in which safety, security, efficiency, and effectiveness can be improved. Ask for their input. "What could be done to make your post more efficient and effective? Do your best to put staff at ease.

When questioning staff, it is important that the audit team be sensitive to the fact that a staff member may be feeling pressured and in a difficult spot. If they seem reluctant to answer, do not push them to respond: move on to another question or to another staff member. Never be critical. Ask questions or discuss; engage staff in conversation.

Avoid comments such as "*You need to...*" "*You must...*" or "*You should...*" Such comments are often felt to be condescending and are beyond the scope of responsibility or authority of the auditor or audit team. Comments about how "*we do it*" should be offered only in discussion in which the staff clearly wish to compare practices or ask for ideas on how they could change their operation. Even then, they should be reminded that any change would have to be authorized by their Warden or Superintendent.

It is important that auditors not record confusing, purely speculative observations that have little constructive value to users of the audit results. Should the auditor's comment be a recommendation for improvement that is not required by policy, he/she/should be clear on that issue.

Do not enter into arguments about your observation. Accept explanations of why the condition is as it is and make note of it but *do not* become judgmental or argue about whether the condition should be as it is. It is the role of the auditor to report the condition: it is the responsibility of the decision-makers to determine it if should be changed.

Although having outsiders looking over ones shoulder will always be a source of some discomfort, auditors can become more safe and positive, and the institution becomes more secure. While not fully in the control of the auditor, the manner in which he/she conducts the audit will contribute greatly to such a positive outcome.

Scheduling Audits

For the first year or two, security audits should be scheduled in advance to enable the institution managers to get accustomed to the idea, avoid scheduling conflicts, and create minimal interference with institution operations. When defensive attitudes and perspectives concerning security audits prevail, advance scheduling is critically important. Such attitudes and perspectives will only change over time as staff come to trust that audits are not being conducted as means of *getting staff*, *catching* the institution in a situation of non-compliance, or to *punish* a facility or staff for problems it has had. If the Department has gained such a reputation, deserved or not, it will take time to develop a positive staff response to the audit process. Clearly announced audits—well in advance of the scheduled date—will go far in alleviating such fears.

It is generally believed that security audits should be conducted at least once each year at each institution. In a large agency, this is a large commitment of time and resources. Some have interchanged *self-audits* and *formal external audits* because of limitations

of resources. If this approach is taken, it is recommended that the audit program begin with the formal external audit to establish expectations. Self-audits should be reviewed by a central security manager with follow-up and assistance in addressing deficiencies. Audits without actions to rectify deficiencies accomplish nothing and establish or reinforce a laissez-faire institution climate.

Audit duration is generally determined by the facility size, security and custody level, and operation complexity. Security audits will typically require a full week, but duration may vary based on the above factors, number and experience of the auditors, and whether there are special issues that must be reviewed.

The presence of auditors in the facility during evening/night hours should be required for the purpose of evaluation of perimeter lighting, observation of housing areas when fully occupied, and opportunity to talk with staff on these shifts and allow them to contribute to the audit. A "real-world" view of the institution must include observation during the hours in which there are fewer program, supervisory, and administrative staff present.

Following the development of an audit program, it is not uncommon for a warden to request an interim audit, sometimes a "surprise" audit. This generally indicates that the program is succeeding and the process is being viewed as non-threatening and helpful. Such requests should be accommodated but audit staff should be mindful that the warden's acceptance of the audit process might not reflect the feeling/attitude of all facility staff. Such audits should be conducted with as much care as initial or annual audits.

When the audit process has been incorporated into the Department's policy and routine operations (usually after about two

years) audits can be conducted on a random, unscheduled basis, if that is the direction the Department chooses to follow. Through a process of conducting a combination of scheduled and unscheduled (surprise) audits, a Department can achieve maximum efficiency and effectiveness in its audit program.

Resources Needed

Properly equipping the audit team will contribute to their efficiency, effectiveness, and contribute to the perception of their competence and preparedness. At minimum, each auditor should be equipped as follows at the time of each audit:

- 1) Notebook containing the following resources:
 - a) Audit policy
 - b) Current agency Security Operations Standards
 - c) Security Audit Instrument
 - d) Notebook, paper
 - e) Institution familiarization packet
- 2) Incidental materials:
 - a) Highlighters, pens, pencils
 - b) Clipboard
- 3) Attire
 - a) Professional, but comfortable clothing (females may want to consider not wearing dresses or skirts when auditing, as climbing stairs, towers, steps, etc., are part of the process)
 - b) Comfortable footwear (lots of walking, climbing)

Some agencies have equipped auditors with laptop computers. This equipment facilitates the compiling of information and development of an audit report. Initially, however, a Department may wish to allow auditors to develop their skills free of the necessity of inputting information from notes taken during the "walk-around" process and so equip them as they become comfortable with the audit process.

Audit Team Site Preparation

To accomplish their work the audit team will need the following accommodations and resources, some of which may have been provided in the preparation packet recommended:

- Designated, private conference/office space to work through the duration of the audit;
- Computer availability in the work area;
- Telephone access;
- Facility schematics and map;
- Inmate handbooks and program descriptions;
- Institution policies/procedures;
- Facility post orders.

The audit team may also request a staff member to be available to escort team members to specific areas, contact staff with whom they need to discuss issues or practices, and assure that other team needs are met. The staff assigned can also provide necessary documentation, as may be requested by the audit team.

It is valuable to the credibility of the audit process and the validity of any subsequent areas of concern noted by the auditors that a staff member from the audited institution accompany the auditors and “see what they see” to better understand the justification for any findings reported.

Pre-Audit Briefing

The audit team should schedule a pre-briefing with the warden and key staff identified by the warden. The pre-briefing should consist of:

- Introduction of audit team members;
- Introduction of facility staff;
- Overview of the audit process;
- Tentative time schedule;
- Discussion of special concerns the Warden and/or staff may have concerning

the audit process or conditions in the institution; and

- Opportunity for the Warden to request special attention by the audit team to a specific area or problem.

It is important that an appointment for a post-audit, verbal debriefing be made at this time. The warden may request and should be given the opportunity to receive a daily debriefing. Other staff may be included in this debriefing as determined by the Warden.

Pre-Audit Tour

The audit team should tour the facility before commencing the audit if the entire team is not familiar with the facility and its programs, architecture, etc. This tour can be conducted on the morning of the first day of the audit. The tour should be short but provide exposure to all areas (i.e. industries, housing areas, education, programs, special housing areas) though the team should not necessarily visit every housing unit, or nondescript areas such as gymnasium, classrooms, etc. The audit does not start during this tour, rather the team is getting the “lay of the land” and a general sense of the condition of the facility. There may be opportunities to ask questions, but they should be limited and attention should be on getting an overview of the facility and its operation. Obvious security related deficiencies should be noted with a plan to explore further after the tour is completed.

As indicated above, the role of the auditor is “to *identify* and *report* (to designated leaders) conditions which in his/her opinion are in variance with agency policy and standards and, in most agencies, *recommend* a more appropriate condition. Experienced auditors will also observe conditions, practices, situations, or problems that are not at odds with policy and standards but which s/he know could be improved.

These should be pointed out—offering helpful suggestions for improvement of the operation.

Security System Checks

We have discussed the role of auditor and the techniques used in conducting an audit. A final technique that is important, both in auditing and in ongoing monitoring of the Institution operations is the security systems check. Briefly defined, a security system check is a simulated emergency designed to test the adequacy of emergency plans and to test staff knowledge, practice, response, and equipment in various situations. To test staff knowledge, practice, response and equipment only in time of actual emergency is courting disaster.

To test staff knowledge, practice, response and equipment only in time of actual emergency is courting disaster.

The purpose of security system checks is, as in other audit activities, to identify areas of risk and vulnerability. Their purpose is *not* to trick staff, rather, to determine areas in which additional training may be require, post orders modified or clarified, procedures changed to address changing condition, equipment upgraded, or supervision strengthened.

A Security system check may be as simple as asking a perimeter staff officer, “What would you do if...?” Or, “What weapon would you use if...?” and “What is the effective range of that weapon?” Or, to determine if the visiting room is searched after a visit, stick an envelope with a note within which directs: “When you find this note, return it immediately to the Captain.” Similarly, a card with a similar directive can be affixed to the perimeter fence to determine if those checking the perimeter are actually giving attention to the fence and its condition. Of course, response and response times to perimeter intrusion alarms, exchanging IDs and attempting to enter the facility, “planting”

a note in a transport vehicle, and a host of other challenges to the security systems can be used.

A program of security system checks should be announced beforehand and an example or two provided so that staff know what to expect. The purpose of the program should be clearly announced and staff informed that discipline will *not* follow staff “failure” of a test. Rather, steps will be taken to improve performance in the future, be that by training, guidance, mentoring, or other types of assistance.

Security system checks should never expose staff or inmates to risk or harm or injury or jeopardize actual institutional security. They should be thought-through and authorized by institution administration. Supervisors should be encouraged to discuss duties with staff on post and question them concerning their knowledge and skills. In authorizing security system checks the following should be considered:

- What is being tested?
- Who should participate?
- Who should have advance notice of the test?
- What safeguards should be in place?
- What specific instructions should be given to the participants?
- How long will the check continue before termination (if applicable)?
- How will the debriefing be handled?

Following a system check, a debriefing should *always* be held with staff involved. Including the institution training supervisor reinforces the administration’s interest in increasing the effectiveness of the training. The employee’s supervisors should be present and members of the administrative team should also participate whenever possible.

Security system checks can be a valuable learning tool, both as part of the audit program and as an ongoing monitoring program. Their judicious use is encouraged to increase staff performance, reduce the routine and boredom inherent in some post assignments, and to address the complacency that invariably creeps into the security operation.

Chapter III

The Audit Report

In order for security systems to reach higher levels of performance, the recommendations for improvement and standards compliance in the audit report must be converted from information to action. Until this occurs, the resources in conducting a quality security audit will not have been utilized to full potential and the audit report may assume, as with many project documents, the familiar position of “gathering dust on an office shelf.”

The report must be treated as an essential ingredient in the organization’s strategic plan to elevate the quality of security systems and practices to the highest-level possible. In order for that to happen, the design must be consistent with the style and needs of the management to be served, and it should be a part of a larger agency emphasis on security performance. For the findings to be translated into improved safety and security, it is essential that there is point-by-point follow through in response to the recommendations.

The security audit report consists of four activities: emergency finds, daily briefings, audit out-briefing, and formal written report.

Emergency Findings

The first of these involves observations that raise an immediate concern for safety and orderly operation of the correctional institution. In the NIC *Conducting Security Audits* seminar, these are referred to as “Oh my god!”—issues that must

be immediately reported to the leadership of the facility for resolution because of the serious risk or vulnerability they represent. Such observations may not become a part of the security audit report—such an incident may be purely idiosyncratic. Nonetheless, follow-up is essential to ensure that the underlying problems have been addressed.

Daily Briefings

During the audit process, the audit team should make itself available to the warden and staff. Many wardens appreciate a daily briefing on audit progress and may correct many deficiencies before the audit team leaves the institution. Priority attention should be given to any special requests made by the warden and the findings and recommendations related to that request should be relayed at the first opportunity. Daily briefings are helpful to the team, as well, enabling them to observe the warden/staff response to the findings and providing insights that may be helpful in delivering the final reports—verbal and written.

Post-Audit Briefing with Warden

The out-briefing is normally held on the final day of the audit and consists of a report on the most important findings of the audit team. The primary deficiencies should be clearly identified in a manner that would allow the institution to move forward with remedies, should they choose to do so, before they receive the written report. Because institutions are often anxious to move forward with improvements, delivery of the written report should be a priority of the audit team and it should be received by the audited

While the audit program and process are important, for the findings to be translated into improved safety and security, it is essential that there be responsible and comprehensive reporting and that the institution and agency ensure that there is point-by-point corrective action in response to the recommendations.

institution shortly after conclusion of the audit.

Especially in new audit programs, it is recommended that the agency's Chief of Security Operations or other Central Office prison administrator be present for the debriefing. Their presence will reinforce agency commitment to the process and underscore the audit team's authority in delivering its findings. It will also provide important feedback to the audit team concerning their performance, manner, and the degree to which their report is consistent with agency expectations. It is important that auditors understand, early in the audit program, their role and relationship with the institution managers. A Central Office administrator can assist them in finding a proper balance in assertiveness and aggressiveness.

The audit team should decide in advance which team member would report on what audit area and plan and rehearse the verbal report to the extent possible. This is especially important in a new audit program and for new auditors. The acceptance of the findings can depend upon the manner in which the information is delivered. Practice makes perfect.

In delivering the report, it is important that phrases such as "*you need to...*" and "*you must...*" be avoided. As said earlier, that is beyond the role of the auditor—the Warden or Central Office administrator will decide if changes will follow the audit recommendation. Rather, the auditor should phrase recommendations as "*the audit team recommends*" or "the audit team suggests." Avoiding first person representation—"I suggest..."--eliminates acceptance or rejection of the idea based on personality and

correctly represents the audit as a team activity and an extension of agency authority.

Hopefully, some "best practices" and other positive aspects of operations have been identified. Staff will have suggested ways in which the operation or their post can be strengthened. These should be mentioned in the report, crediting responsible staff, by name. A balance of positive findings with deficiencies will be helpful in gaining acceptance of the recommendations.

Time should be allowed for questions and comments from staff but argumentative discussion should be avoided. The report consists of auditors' observations and recommendations – no decision has been made as to their acceptance. Auditors may provide rationale for their position but should not enter into argumentative discussion of the merits of the existing condition.

When giving the verbal report, be kind but honest. Do not "gild the lily." Do not be *redundant* in praise to balance things that are difficult to say. It will be viewed as phony—rightly so.

The Written Report

The audit report format will ordinarily be determined by the format of the Security Audit Instrument used by the agency. The report format design, in addition to including specific findings relative to security operations, should also include space for general comments concerning topics such as the general atmosphere of the facility, sanitation, staff morale, the mood of the inmate population, and the overall quality of the organization.

Narrative Instrument:

When a narrative instrument is used, the report will consist of a narrative listing of

When giving the verbal report, be kind but honest. Do not "gild the lily."

observations and recommendations for each/most of the deficiencies noted. Because the narrative format does not contain an exhaustive listing of points of review, other observations or issues will also be noted, often as *Special Issues* with a recommendation for each. These should, for ease of reference, follow an uninterrupted, numerical sequence from the beginning to the end of the report. This feature also helps eliminate confusion when the report is quite extensive, containing many observations and recommendations. This format is simple and straightforward... (see *Attachment #1*). An advantage of this format is that when completed, the audit report contains only issues where risk and vulnerability have been identified. A report "by exception" format reduces report volume and serves to emphasize the issues needing attention.

Tabular Instrument:

When a tabular instrument is used, the audit report will normally be in the form of a chart or summary checklist (see *Attachment #2*). The report will normally contain an indication of compliance, non-compliance, etc., for each of several hundred individual standards-related points of review. Similar to the narrative instrument, the information will be organized according to basic security topics (searches, visitation, key control, etc.). The tabular report tends to be quite voluminous and may tend toward a checklist outcome without much helpful information unless the auditors are highly skilled and knowledgeable in security matters and have experience working with this audit instrument, which demands great attention to specific detail.

Since the format of the report is largely driven by the security audit instrument, it is important that the agency carefully consider the outcome that will be most useful to them when they select or design a security audit instrument. Whatever the choice, it should be consistent with the resources of the agency, the skill of the auditors who will be conducting the audits, and it should be user-friendly to the people it serves.

Audit "Scores" or "Rankings"

In our competitive environment we have a natural tendency to "score" things. "How did we do?" is a normal question following an audit. A typical response is often in the number of deficiencies or areas of non-compliance. In some instances a score is tallied following each audit and institutions are "ranked" according to their score.

Scoring and ranking are meaningless... Having a security audit scored or ranked may be likened to the value of knowing the "average depth" of a river: one can drown in a river with an average depth of six inches.

Scoring and ranking are meaningless when related to security auditing. Having a security audit score or rank may be likened to the value of knowing the "average depth" of a river: one can drown in a river with an average depth of six inches.

Consider this example: The first ranking institution—best score—has 2 deficiencies. The second ranking institution has 10 deficiencies. The first ranking institution's deficiencies are in the area of Class A tools and pose serious threat to the security of the institution and the physical well being of staff and inmates. The second ranking institution's 10 deficiencies are in the area of handling of inmate mail, property and laundry: none being of a serious nature. Can it truly be said that the first institution is a "better" institution or had a better audit outcome than the second?

The writers of this document are unaware of any benefits in scoring and ranking. There are several problems that should be considered before authorizing the scoring or ranking of audit outcomes. Scoring and ranking tends to do the following:

- Undermines the stated purpose of a healthy audit program: to learn of risk and vulnerability and improve the safety and security of the facility. The focus invariably turns from substantive issues related to safety and security to that of numerical outcomes and/or competition.
- Reinforces fears that audits are to “catch” staff/institutions doing wrong and perhaps, find cause to punish staff.
- Reinforces a culture of suspicion and resistance around audits.
- Leads to “cover-ups” and diminished cooperation with auditors.
- Leads to “pay backs” as staff audit each other’s institutions.
- Creates an “earning” culture rather than a “learning” culture.

A “win—lose” audit culture is a culture in which there are no winners. It is almost certain to diminish the value of audits as staff focus on the score and rank rather than on discovery and correction and creates a downward spiral in audit effectiveness.

Executive Summaries

The full audit report delivered to the institution and central office at the conclusion of the site visit can be quite voluminous. It can contain many pages simply reporting that the facility is compliant with specific standards. Executive staff are extremely busy people. Documents for them need to be reduced to the essence of important information in a user-friendly format.

It is suggested that the original report be reduced to include only reports of “non-compliance” and, if applicable, “essentially

compliant,” and standards which are compliant that include reference to exemplary practices. In addition, recommendations for improvement in practices that are not violations of policy standards should be included.

The report derived from a narrative format instrument is essentially, an executive summary including primarily those issues in which action is recommended for improvement. Care should be given to ensure that the issues are properly ordered, with a table of contents, clearly articulated, and a section added to each issue in which the warden can indicate his/her plan or action.

If system wide action is recommended, issues from all institutions can be collapsed into a single report to reflect the overall agency status/need as related to a specific security topical area.

Report Distribution and Follow-up

Report distribution requirements vary among agencies. However, the full audit report, with executive summary if required, should normally be delivered to the institution within 2 to 4 weeks following the conclusion of the audit. The institution should be expected to develop complete action plans addressing each area of deficiency within a reasonable time thereafter, submitting it with a copy of the audit report (or executive summary) to agency executive staff. The action plan should include information concerning resources required to implement audit recommendations and a time-line for each of the proposed changes/improvements.

If the institution disputes any of the findings, these are normally appealed to the Chief of Security Operations for a final determination to be made.

A copy of the audit report (executive summary) and action plan is provided to the audit team at the time of the next audit.

Legislative/Gubernatorial Reporting

One of the best indicators of a quality organization and a pro-active approach to success is that members have the same degree of commitment and a shared understanding of critical issues at all levels of the organization. In a correctional organization few disagree that quality security is a critical issue. A pro-active, forward-looking correctional security

program should include an annual security report to key legislative agents and, in state agencies, the Governor's office. It can become the basis of uniting all players on very important security issues.

This type of report should be very general in nature, outlining the security concerns and accomplishments of the performance year for the Department (*see Attachment #3 as an example*). A separate budget line for security hardware, equipment, and systems can be a very productive companion to this version of the audit report.

Confidentiality

The audit report is likely to contain recommendations for improvement and indications where security is not performing at its best. Obviously, it could be very damaging should it fall into the hands of inmates. Therefore, it should be utilized and stored in areas where inmates may not have access under any circumstances. Additionally, the report may be something in which the media or private interest groups have a keen interest. In some circumstances it may be an advantage to the Department for them to know the content. However, it must be remembered that all of the media or private interest groups can become adversarial at any

time. Any part of the report could be used in that experience. The best policy is to not make reports available outside the correctional department except by court order or the discretion of the executive director.

Action Plans

As indicated earlier, the audit report should contain a comments/action plan section in which the Warden can note the desired action. Where the audit report indicates a condition, which is non-compliant with respect to performance standards, or a general condition that could be improved, the

One of the best indicators of a quality organization and a pro-active approach to success is that members have the same degree of commitment and a shared understanding of critical issues at all levels of the organization.

decision to act should be recorded as the action plan for that standard. Audit policy should direct that the action planning be a collaborative process by which facility staff

consider possibilities and select strategies for achieving success. The results would list steps for implementation, persons responsible for each aspect, and expected completion dates.

Conclusion

The audit report should be designed to be compatible with a larger departmental effort to achieve the highest levels of security. The format should be efficient, user friendly, and provide enough information to be useful to the facility or organization to be served. It should be a modified version of the audit instrument. The modification should fully integrate the standards being audited, the conclusions of the auditor, helpful clarification, and an action plan to improve security program operations. Under an umbrella of confidentiality, the report should be distributed and made available to key corrections and governmental staff that have a direct role in managing the organization.

The written report must never be a significant departure from the informal out

briefing provided to the Warden and staff. When the written report is delivered, there should be no major surprises. A security audit report, responsibly completed and delivered can, and should become a welcome "to do" list which, when completed, will add to the safety and security of the facility.

Although the report and follow-up activity is an important outcome, it is important to recognize that much benefit is gained in the audit *process*. The attention to policy, procedure, standards, post orders, staff, operations, equipment, and facility all bring tremendous attention to the importance of sound security standards and practices. But, attention to a formal written report and the development of an agency supported action plan, with resources provided where needed and possible, are "frosting on the cake" and a powerful force in the ongoing development of safe and secure institution operations.

NARRATIVE SECURITY AUDIT INSTRUMENT FORMAT

14.03.01 *There is written policy establishing an automation security workgroup to review all requests to grant inmates use of computers and computer technology as part of their work or study assignment.*

Observation:

There is no computer security workgroup

Recommendation:

Establishment of such a group with first mission to develop local policy and oversight procedures of inmate computer access.

14.03.06 *Audits of all inmate computers are conducted at least quarterly by knowledgeable staff to prevent abuse or unauthorized use of the systems.*

Observation:

No such practice of computer review is in evidence.

Recommendation:

See 14.03.01

Key Control

16.01.03 *A staff member is assigned to assist the locksmith and to provide backup assistance in the absence of the locksmith or during institution emergency.*

Observation:

Sgt. XXXX is the only trained locksmith at the facility and is not currently on pager for an emergency response.

Recommendation:

Select and train a backup locksmith for the facility and provide a pager for the current locksmith to facilitate his response to the facility in a timely manner in case of emergency.

16.01.03 *There is a position description and current post orders that describe the duties and responsibilities of the locksmith and locksmith assistant.*

Observation:

The current locksmith Sgt. XXX is also responsible for tool control, pest control and fire safety. These assignments encompass a vast area of responsibilities in the facility. There is no post order for these functions.

Recommendation:

Develop a post order that would clearly define the scope and parameters of this individual's duties and responsibilities within the institution.

Special Issue:

Sgt. XXX is an outstanding employee who has shown a high level of skill and commitment and should be commended for all the duties in the facility for which he is currently responsible. He created the lockshop, including use of his personal equipment for key cutting, pinning, stamping, etc. He created a fire response capability of six inmates, trained them, and has carts with all response equipment immediately available. He also created on his computer a manual for evacuation codes, one of the most comprehensive specific documents this team has ever seen. Great job, great employee.

16.03.01 *All keys are returned to the issuing location at the end of the workday or when the employee to whom the keys were issued leaves the institution.*

Observation:

The team is concerned that the facility does not have a central area to issue facility keys to staff. They are issued from various areas within the facility to the staff assigned to the area. The concern would be accountability, non-current inventories, broken or lost keys. Staff on units exchange keys, but they do not exchange key chits.

Recommendation:

Issue keys from central area such as Post #1. Utilize the chit system.

For assignments, keys are exchanged and do not leave the post. Procedures should explain how to exchange chits. In units where keys are exchanged from one staff to another, the exchange should be noted on shift log with number of keys exchanged and staff key chits maintained in the officers' area.

16.04.12 *A record of the issuance of restricted keys is maintained bearing the key ring number, date, time of issue and return, the person whom issued, the purpose of the issue, and the person authorizing the issue.*

Observation:

The locksmith's two sets of duty keys (highly restricted) are issued and turned in at Post #1. No procedure is in place for preventing these keys to be issued to anyone who requests them.

Recommendation:

The use of a sequence lock for these sets and all restricted key sets with a log maintained of all key draws authorized to others on restricted keys. Sgt. XXX is implementing a color chit system, which will eventually assist in addressing this issue.

Perimeter Security

18.01.01 *There is a written department policy that designates a security level to the institution and specific perimeter design/construction requirements related to that security level.*

Observation:

No policy could be found that designated specific perimeter design/construction requirements

Recommendation:

Due to multi-levels of custody in this institution, specific guidelines should be maintained for a minimum level of perimeter design including double fencing, razor wire attachments to gates and adjoining fences and lockdown features on electric gates.

18.01.02 *There is written institution policy that establishes a requirement and procedures for continuous surveillance of the institution perimeter.*

Observation:

No written policy requires continuous surveillance of the perimeter

Recommendation:

Whenever possible, a 24-hour moving patrol should be implemented along with a vindicator mapping system for sufficient surveillance of the perimeter and rapid response to zone of alarm. Policy should describe the specific method by which continuous surveillance is maintained.

18.01.03 *There is an electronics technician on staff and/or on call who is formally trained in the maintenance and repair of all perimeter electronic detection systems and other electronic equipment in use in the institution.*

Observation:

There are personnel who can be called in at all times to repair systems for perimeter detection but certain staff voiced concerns that insects (spiders) could cause system to malfunction.

Recommendation:

More visual checks of equipment on a routine basis should eliminate this problem

18.02.02 *The number of inner and outer razor rolls and the type of barb used (long or short) is appropriate for the perimeter security category of the institution being reviewed.*

Observation:

The number of inner and outer razor rolls were inconsistent along several areas of the fence. Double fencing was available in some zones but not in most. Ground razor wire was along inner fence in some areas and should be at inside bottom of the entire outer perimeter fence.

Recommendation:

The team recommends that facility security fencing be reviewed and a decision made concerning the minimum level and configuration of perimeter fencing acceptable and that the entire perimeter be upgraded to this level and configuration.

18.02.04 *Perimeter lighting between the fences and thirty (30) feet on either side provides low-light vision and complies with department standards.*

Observation:

Perimeter lighting was sufficient in most areas and provided good low light visibility. Two areas inside the institution were considered to be problematic at Pin Bluff unit and the back of horticulture area.

Recommendation:

Provide lighting in area adjacent to horticulture building for added visibility and to front side of Pine Bluff dorm adjacent to HVAC systems. Remove or relocate the wooden shed in back of Horticulture area—blocks visibility and light.

TABULAR SECURITY AUDIT FORMAT

Attachment 2

Function	AR 300-8 Key/Lock Control				
AUTHORITY	AUTHORITY REQUIREMENT	EX	C	E C	NC
SEC.III.N.3	The following areas shall have access by Restricted Keys:				
SEC.III.N.3.a	▪ property storage		X		
SEC.III.N.3.b	▪ evidence storage		X		
SEC.III.N.3.c	▪ armory		X		
SEC.III.N.3.d	▪ medical department		X		
SEC.III.N.3.e	▪ primary issue point for keys		X		
SEC.III.N.3.f	▪ administrative offices		X		
SEC.III.N.3.g	▪ perimeter fence gates		X		
SEC.III.N.3.h	▪ other critical areas as designated...Administrative Head...facility ▪ Check and observe restricted keys. ▪ Are all categories listed treated as Restricted keys? ▪ Review restricted key sign-out log; compare to key box.		X		
SEC.V.A.1	From the Primary Issue Point, the Key control officer shall issue essential key rings to secondary issue points. Secondary issue points shall be determined by the Administrative Head of the facility. ▪ Are these points identified in written policy and procedure?			X	

DEPARTMENT OF CORRECTIONS SECURITY LEGISLATIVE REPORT

State statute requires the Director of the Department of Corrections to, at a minimum: conduct or cause to be conducted announced and unannounced comprehensive security audits of all state and private correctional facilities. In conducting the security audits, priority shall be given to older facilities, facilities that house a large proportion of violent offenders, and facilities that have experienced a history of escape or escape attempts. At a minimum, the audit shall include an evaluation of the physical plant, landscaping, fencing, security alarms and perimeter lighting, and inmate classification and staffing policies. Each correctional facility shall be audited at least annually. The Director shall report the general survey findings to the Governor and the legislature.

To this end, the Director initiated an unannounced security audit process augmenting the security component of the existing management review process. An audit team comprised of individuals with extensive and diverse institutional security experience was formed to operate out of the Department's Bureau of Security Operations.

The process utilizes regional and facility personnel to conduct announced audits of half the Department's facilities annually. The unannounced audit team is responsible for conducting audits of the remaining facilities and adjoining units. Great care is taken to maintain the confidentiality of the selected audit locations and NO advanced notice is given. The Wardens and facility staff are only advised of the audit following the arrival of the team. This facilitates a more accurate, realistic picture of the day-

today security operations and provides for a better assessment to identify deficiencies and security needs. The first audit utilizing the new process was completed December 21, 1995. Since that time a total of 34 audits have been completed.

The audit instrument used by the audit team contains 238 standards, which were primarily derived from existing policy requirements. Facilities are required, at a minimum, to comply with these standards. The audit process also considers other areas not necessarily covered in the audit instrument relating to the security systems of the individual facilities with unique mission requirements. The audit instrument is subject to revision and additions based on the identification of new areas of concern, as well as best practices developed at specific institutions and noted for special mention. Deficiencies in the physical plant that might impact security are also reported.

Upon completion of an audit, a detailed report is submitted. This report lists the deficiencies discovered during the audit as well as recommendations for how they are to be corrected. This information is then shared via security advisories disseminated statewide to all facilities in an effort to ensure consistency and promote continued improvement of our security systems. Upon receipt of the audit report, Wardens are required to submit a corrective action plan to the Director of Prisons within 30 days. Random unannounced follow-ups are then conducted by the audit team to ensure the corrections listed in the action plan have taken place.

The most common findings noted during the unannounced audits this reporting period were in the following areas:

- (Weapons) Issue logs not properly filled out
- (Keys) Key Tag with hook code and number of keys inaccurate
- (Entrance Procedures) All purses/packages not searched
- (Tools) All tools not etched and double color-coded for accountability
- (Tools) Each shop not keeping perpetual tool inventories
- (Tools) Inventories not maintained in required format.
- (Sensitive Items Control) Inventories not properly maintained
- (Sensitive Items Control) All poisonous/Toxic fluids not secured when not in use
- (Transport) Armed transport officers not consistently issued ERDs

The majority of these deficiencies *were performance related* and not reflective of the security system. Nevertheless, corrective action was taken in all such cases and documented. Accountability systems were evaluated and strengthened as necessary to guard against recurrence.

The most commonly encountered *physical plant deficiencies* pertained to:

- Perimeter lighting not meeting established standards
- Perimeter fencing corroded
- Erosion in the area underneath the perimeter fence
- Lack of internal cross fencing needed for inmate control
- Malfunctioning locking mechanisms

Subsequently, all the above physical plant deficiencies were evaluated and a corrective action plan for each developed in

conjunction with the appropriate cost proposals.

In addition to the areas indicated above the current radio communication system has also been identified as a major security concern. Good communications is an essential element of our overall security system. Some of the most prominent problems being encountered with our current system are:

- Limited range
- Interference caused by having numerous facilities in close proximity of each other
- Low band radios will not transmit/receive properly from within the new reinforced concrete buildings we are currently constructing

It should also be noted that our present radio system has never been updated. In order to remedy these and other problems and keep pace with changing needs, a plan to implement the 800 MHz system designed for law enforcement and correctional use has been developed. We are optimistic that we will have this new technology in use throughout the department by the year 2000.

This audit process emphasizes innovative and new approaches employed by some facilities that have statewide implications. One of the most positive aspects of this process comes from sharing this information. Again, the process recognizes that our most valuable resource is our staff. Auditors also conduct "system checks" such as activating fence alarms to observe staff reaction to mock escape attempts, testing emergency equipment to ensure it is properly maintained and operational, and quizzing staff relative to various scenarios to ensure they are properly trained to react to emergency situations. The auditors approach

“system checks” by attempting to think like inmates to exploit or defeat the security system of a facility. This is done not to embarrass staff but to illustrate weaknesses in the system.

With the advent of the unannounced audit process, a dramatic decrease in the number of escapes has been noted. There have been 2 escapes from a secure perimeter during the current fiscal year with 6 during fiscal year 95-96 as compared to 21 in fiscal year 94-95. We are confidently moving toward our expected goal of *zero* escapes from secure perimeters. Significant improvement in facility security systems has also occurred, as well as a heightened awareness among all staff (not just security) that *“Quality is contagious and security is our number 1 priority.”* As a result of the overall success of the unannounced security audits, plans are underway to expand the process to cover all facilities annually.

Chapter IV

The Security Audit Instrument

■ How to Use the Security Audit Instrument

This security audit instrument has been used during the audit of numerous host institutions to the NIC *Conducting Prison Security Audits* training seminars. Numerous changes have been made based upon the experience of the participants, the "best practices" of the facilities and the auditing team leaders. Although it includes many of the essential elements of a sound security program, the instrument is not designed or intended to meet the final audit requirements of any agency or institution until it has been tailored to that agency or institution's specific needs and requirements.

There is no "one size fits all" in the world of audit instruments. Existing instruments range from those that are policy based with little attention to practice to those that are fully based in the detail of security practices. There is also variance in content because there are differences in security standards and operations among correctional agencies and differences in what various institutions have decided to audit. However, there are many similarities in core security principles and practices. Recognizing this, this instrument was developed as a "model" that incorporates many/most of those essential elements and can serve as a foundation document that can be adapted to state and institution security policies, procedures, standards and practices:

- One of the differences among correctional agencies is in *terminology*. The terms used in your audit instrument must reflect the common usage and understanding in you agency.

- Other differences are in written *policy* and whether there *is* written policy (by design or oversight). The security audit instrument is intended to be suggestive of policy: that is, it inquires about written policy in those areas in which most security specialists believe written policy should exist.
- Not only does "what" agencies require differ, but "how" it is to be accomplished varies. Thus, written *procedures* differ among agencies and it is essential that the audit instrument be adapted to reflect the expectations of the agency.
- Agencies also vary in *standards*: the minimum level of performance or response to a policy, issue, or problem. Whether the standards are internal or external (statutory, ACA or other), they should be reflected as points of review in the adapted audit instrument.
- There is also significant divergence in *practice* based on many factors, including the mission of the institution, levels of staffing, available supervision, and physical plant. In adapting the instrument, such factors must be considered.

This audit instrument is a *starting point* for the development of a comprehensive audit instrument. Though some may choose to use it as is or with minor alterations, its best use will come through careful adaptation to more nearly incorporate the individual agencies' security philosophy as reflected in its policy, procedures, standards, and practices.

All Persons Participating in the Security Audit Process Should Read the Following Thoroughly Before Proceeding.

Before conducting an audit, whether using this instrument or a fully adapted version, each auditor should understand the following:

1) This security audit instrument, like all others, is not all-inclusive. There are many security details that are not in the instrument that are very important to the security of an institution.

The security audit instrument will bring the auditor to the areas/issues in which potential security lapses may occur. It is important that each auditor have extensive security experience that enables her/him to recognize security weaknesses or deficiencies within the myriad of detail that comprises institution operations.

2) **The task of the auditor(s) is fact-finding: the Warden and/or his/her staff and superiors determine error or need for change.** If the auditor cannot give a positive response at each Point of Review, it should *not* be inferred or suggested that the institution/agency is in error or that the security of the facility is in jeopardy: the auditor should simply state the observation. An institution/agency may have thoughtfully decided, for good reason, not to require by policy or in practice certain broadly held security practices. If such a decision *seems to the auditor to create a potential risk situation*, that should be noted with a recommendation that the institution/agency decision and practice be reviewed. Similarly, if written policy and/or procedure is lacking or inadequate, or staff knowledge and security practices suggest the potential for a breach of security, this should be clearly communicated in the audit process. *Critical deficiencies; those that, in the opinion of the auditor, could create an immediate risk to safety or security,*

should immediately be brought to the attention of institution managers.

- 3) Auditors should recognize that institutions of differing security or custody ratings, program objectives, architectural structure, staffing complement, or inmate profile may present different risk characteristics. An apparent deficiency in one institution may be more critical than in another. *However, security deficiencies should not be passed over because they seem to be less critical because of the custody level, etc.* All deficiencies should be identified and reviewed by those who are responsible for the security of the institution.
- 4) A security audit that is not thorough, thoughtful, and conducted by credible persons can have the opposite impact of that intended.
- 5) An audit that “glosses over” security deficiencies and/or fails to report them may suggest to staff that the issues are not of significance and give a false sense of security.
- 6) If the audit is not done carefully and accurately, misleading findings or recommendations may be made and the audit report “discounted” or ignored.
- 7) If the persons conducting the audit are not experienced and credible, the report and recommendations may not be viewed as credible.
- 8) If an audit is conducted with a “gotcha” attitude, staff may be uncooperative, resistant, and even hide potentially serious deficiencies in fear of disclosure and possible discipline.

The timeworn work adage might be paraphrased as follows: “if a security audit is worth doing, it’s worth doing well.” Given the consequences of poorly conducted audits, we might better counsel that security audits be conducted *only* if they can be conducted in a thorough, careful, thoughtful, and instructive manner by experienced persons.

The Security Audit Instrument:		Page
Section 01	Armory/Arsenal	39
Section 02	Communications	44
Section 03	Inmate Counts	47
Section 04	Control Center(s)	50
Section 05	Controlled Movements	54
Section 06	Use of Force	56
Section 07	Hazardous Materials Management	60
Section 08	Inmate Mail	63
Section 09	Inmate Visiting	65
Section 10	Inmate Property	69
Section 11	Inmate Work Assignments	72
Section 12	Inmate Transportation	76
Section 13	Key Control	81
Section 14	Perimeter Security	91
Section 15	Physical Plant	100
Section 16	Post Orders	104
Section 17	Searches	106
Section 18	Security Inspections	113
Section 19	Segregation (Special Management)	116
Section 20	Tool and Sensitive Item Control	122
Section 21	Emergency Plans	131

01. ARMORY/ARSENAL

Objective: *To provide secure storage, handling, and accountability for firearms, ammunition, chemical agents, and security equipment.*

Points of Review:

01.01 Responsibility

01.01.01 There is written policy that establishes responsibility for operation and supervision of the Armory/Arsenal and procedures for safe and secure management of armament and supplies.

Observation:

Recommendation:

01.01.02 There is written policy that limits access to the armory to those persons with an official need to be there. Only those staff designated in writing by the warden or superintendent may enter unaccompanied.

Observation:

Recommendation:

01.01.03 A staff member is designated by the Warden/ Superintendent as the “armorer” and assigned responsibility for operation of the Armory/Arsenal.

Observation:

Recommendation:

01.01.04 Staff authorized to issue and receive weapons are certified (trained) in use of those weapons. Current, written documentation of those certified is maintained in the armory and at all other weapons issue points. Weapons cards may be required and exchanged in the same manner as “chits” when weapons are issued.

Observation:

Recommendation:

01.01.05 Written policy establishes the Warden/Superintendent as approving authority for issuance of weapons and for the carrying of weapons into the institution.

Observation:

Recommendation:

01.01.06 A staff member is assigned to assist the armorer and to provide backup assistance in his/her absence or during institution emergency.

Observation:

Recommendation:

01.01.07 The armorer and assistant armorer have received training in all duties pertaining to the operation of the armory/arsenal including weapons maintenance.

Observation:

Recommendation:

01.02 *Records and Documentation*

01.02.01 There is a current master inventory of all firearms, munitions, chemicals, and security equipment. Munitions are recorded by make, type, caliber, and serial number. Firearms are recorded by serial number, brand name, and assigned location.

Observation:

Recommendation:

01.02.02 There is department policy requiring standardization of armory equipment in all institutions with a specific listing of all such equipment either included or referenced to another document approved by the appropriate agency authority.

Observation:

Recommendation:

01.02.03 An entrance logbook is maintained bearing the signature, date, time of entrance, time of exit, and purpose of the entry of all persons entering the armory. Entrance should be by restricted keys or other secure access system.

Observation:

Recommendation:

01.02.04 A written record in the form of a secure sequential log is maintained of the routine and emergency issue of any security equipment from the armory.

Observation:

Recommendation:

01.02.05 Firearms; ammunition, chemical agents, and defensive, detection, and communication equipment are inspected at least monthly and an official inventory made at least once each month. All armory equipment inventories are perpetual with a new balance established at the conclusion of each adjustment. The chief security officer of the facility will review each of these inventory reports.

Observation:

Recommendation:

01.02.06 A sub-inventory is maintained in all areas where firearms, munitions, and/or chemical agents are assigned/stored.

Observation:

Recommendation:

01.02.07 The expiration date of chemical agents is etched or otherwise indelibly marked on the container upon receipt. There is consistent rotation of chemical agents.

Observation:

Recommendation:

01.02.08 There are written logs/ reports of inspections indicating that all firearms and defensive equipment are cleaned, test fired, and functioning properly. All weapons are inspected at least semi-annually and unserviceable weapons are repaired or replaced.

Observation:

Recommendation:

01.02.09 All weapons inventories, storage, and issue logs are current, legible, and correctly filled out.

Observation:

Recommendation:

01.03 *Armory/Arsenal: Facility and Operation*

01.03.01 All firearms are clean, securely stored, tagged appropriately and are in good condition.

Observation:

Recommendation:

01.03.02 Chemical agents of different types are stored separately, clearly marked to indicate expiration date. Expired chemical agents are clearly distinguished from the current inventory by storing them in separate location within the arsenal and clearly labeling them as expired.

Observation:

Recommendation:

01.03.03 Body armor shells/carriers are washed prior to reissue and are in good condition.

Observation:

Recommendation:

01.03.03 If personal weapons are authorized for storage in the armory/arsenal, measures are taken to ensure they are unloaded, properly secured and stored in an area away from state owned weapons. Single-weapon vaults are provided for storage.

Observation:

Recommendation:

01.03.05 Written policy prohibits unauthorized persons carrying weapons into the institution. Provision is made to store law enforcement officers' weapons and ammunition before entering the institution.

Observation:

Recommendation:

01.03.06 Practice was observed that demonstrated compliance with policy related to the safe storage, issue, handling, use, and return of weapons.

Observation:

Recommendation:

01.03.07 The institution is in compliance with department policy requiring the standardization of security equipment.

Observation:

Recommendation:

01.03.08 The design and construction of the armory/arsenal meets or exceeds the following physical specifications:

- Entry door is of solid construction: at least 12 gauge steel. A secure pass-through or split door with security screening is provided to facilitate the issuing of armament.
- High security locking mechanism.
- Floors, walls, and ceilings are of steel reinforced concrete material with no false ceilings or panels.
- If there is no sally port, additional security precautions are taken to prevent unauthorized entry.
- Appropriate humidity and ventilation controls, emergency lighting, telephone, and radio communications are provided.
- Appropriate space is available for weapons, munitions, and equipment, and space for maintenance, distribution, and documentation.
- Metal storage cabinets are provided for the storage of ammunition.
- The arsenal is located outside the security perimeter.
- A safe bullet trap for loading/unloading of weapons is located at the entry.

Observation:

Recommendation:

02. COMMUNICATIONS

Objective: *To provide secure and efficient contact with staff in and outside the institution and law enforcement agencies to facilitate effective supervision of inmates and ensure the health, safety, and security of staff, inmates, and visitors and protection of the community.*

Points of Review:

02.01 Responsibility

02.01.01 There is written policy that establishes responsibility for radio assignment for each person/post in the communication network and for supervision and maintenance of communication equipment and operations.

Observation:

Recommendation:

02.02 Equipment

02.02.01 The use of personal communication equipment (radio, cell phone, etc.) is strictly prohibited. Possession of personal communication equipment is prohibited within the secure perimeter of the institution.

Observation:

Recommendation:

02.02.02 All communication systems and equipment comply with department standards.

Observation:

Recommendation:

02.02.03 There is an adequate number of portable radios, a battery recharge station, and a system in place for repair/replacement of equipment. Radios are in good operating condition.

Observation:

Recommendation:

02.02.04 The number of serviceable radios complies with the agency/institution standard. If not, the purchase has been initiated or a plan developed to procure additional radios or replace any that are non-serviceable.

Observation:

Recommendation:

02.02.05 Institution vehicles are equipped with a vehicle radio in good condition.

Observation:

Recommendation:

02.02.06 Each security post has at least one means of direct communication with the control center.

Observation:

Recommendation:

02.03 *Communication System Operations*

02.03.01 All communication equipment, including duress alarms and emergency telephone systems, is tested at the beginning of each shift from the post/area from which they will be used.

Observation:

Recommendation:

02.03.02 A current, printed list of radio ten-codes/call numbers (if used) is posted in a prominent place near the base station in the control room.

Observation:

Recommendation:

02.03.03 Ten-codes/signals are appropriately utilized when using institution radios.

Observation:

Recommendation:

02.03.04 A coded system is used by the control center for communication with community work crews. Institution work crew supervisors routinely notify the control center of their general location.

Observation:

Recommendation:

02.03.05 If the institution has multiple units (annexes, work camps, outside warehouses, etc.), each unit has been assigned distinctive unit descriptions for staff who are assigned hand- held radio units and there are no repetitive ten-codes/signals, descriptions, or duplicate unit designations which could create confusion during emergency situations.

Observation:

Recommendation:

02.03.06 Security officers in non-stationary or non-visible positions routinely notify control center staff of their general location in the institution or off grounds.

Observation:

Recommendation:

02.03.07 All staff receive proper radio communications training that is documented indicating the date attended and competencies attained. Staff practice demonstrates competency.

Observation:

Recommendation:

03. INMATE COUNTS

Objective: *To provide accountability for the entire inmate population at all times and at all locations to prevent escape and ensure a safe, secure living/ working environment and the safety of the general public.*

Points of Review:

03.01 Responsibility

03.01.01 There is written policy that establishes procedure for the scheduled, informal, and emergency counting of inmates and for recounts in the event of a miscount.

Observations:

Recommendation:

03.01.02 In order to ensure accuracy in accounting for inmates, written policy limits “out counts” to the absolute minimum number necessary

Observation:

Recommendation:

03.01.03 “Out counts” are approved by the shift commander in advance of count time.

Observation:

Recommendation:

03.01.04 The final inmate count is approved and signed by the shift commander before a “count cleared” indication is given.

Observation:

Recommendation:

03.01.05 All institution staff are trained in inmate count procedures and their responsibility relative to the accounting for inmate whereabouts. Staff are monitored to ensure that they are conducting frequent, informal counts of inmates under their control.

Observation:

Recommendation:

03.02 ***Count Procedures***

03.02.01 There are at least 6 six formal counts in a 24 hour period of which two counts are mandatory standing counts.

Observation:

Recommendation:

03.02.02 There is at least one scheduled (formal) morning count conducted before inmates begin checking out of housing areas for scheduled activities.

Observation:

Recommendation:

03.02.03 There are at least two staff counting the same group of inmates in each count area. Preferably one officer/staff maintains a position where the entire group being counted can be observed to prevent movement of any kind.

Observation:

Recommendation:

03.02.04 It is required that all inmate movement cease from the time count is announced until the count is cleared.

Observation:

Recommendation:

03.02.05 It is required that industries, construction, and delivery vehicles that cannot be easily searched be locked and remain in the institution until a count has cleared.

Observation:

Recommendation:

03.02.06 Staff are required to count only living, breathing flesh.

Observation:

Recommendation:

03.02.07 Staff conducting count do not allow distractions while in the count process nor do they routinely perform any others duties during this time. Staff do not take phone calls during count. Inmates who distract staff during count activities are considered to have committed a major violation of institution order and are subject to major sanction.

Observation:

Recommendation:

03.02.08 Inmate participation in any portion of count activity is prohibited, including preparation, processing, delivery of count slips, or handling of count related documents.

Observation:

Recommendation:

03.02.09 Security staff are required to provide up-to-date information to designated staff who are responsible for the master count concerning all housing moves, transfers, releases, and other activity that may impact the master count and accounting for inmates.

Observation:

Recommendation:

03.02.10 All count slips, tabulations, and master count sheets signed by staff conducting count, tabulating count, and clearing count, are maintained on record for a minimum of 30 days.

Observation:

Recommendation:

04. CONTROL CENTER(S)

Objective: *To facilitate the secure management of security systems, including keys, communications, inmate and staff movement, emergency supplies, and other security equipment and control access and egress to the facility or area of responsibility.*

Points of Review:

04.01 Responsibility

04.01.01 There is written policy, procedure, and/or post order limiting access to the control center(s) specifically to those persons with official need to enter.

Observation:

Recommendation:

04.01.02 There is written policy, procedure, and/or post order specifically indicating persons to whom keys may not be issued. This includes inmates, off-duty staff, volunteers, visitors, vendors, and may include part-time and contract staff.

Observation:

Recommendation:

04.01.03 Written post orders detail control staff responsibility related to:

- communication with vehicles in transit, work crews, and others;
- management of emergencies including fire, disturbance, hostage situation, inmate strike, escape, power failure, or other emergencies;
- issuance of keys, emergency equipment, emergency supplies, etc.;
- identification procedures related to facility entrance or exit.

Observation:

Recommendation:

04.01.04 Written post orders include a comprehensive hostage situation statement, such as: "No person under duress retains authority to give orders or direction to any staff member" and "No inmate will be released with hostages".

Observation:

Recommendation:

04.02 *Operations*

04.02.01 Secure space and accommodations are provided for twenty-four hour (24) hour control center operations. Communications, access and egress may be controlled from this area.

Observation:

Recommendation:

04.02.02 The institution maintains an effective communication system that provides instant communication between the control center and offender living areas, security posts, all areas of the facility and mutual aide agencies.

Observation:

Recommendation:

04.02.03 Control center staff are conversant with initial emergency response responsibilities, including response to electronic alarms, initial staff notification and callback, and issuing of emergency equipment (test).

Observation:

Recommendation:

04.02.04 Current, legible logs are maintained documenting the issue and retrieval of emergency and restricted keys, weapons, restraint and control devices, chemical agents, and other emergency equipment and supplies maintained per existing policy (observe/review).

Observation:

Recommendation:

04.02.05 Key control procedures are consistently followed, including requirements for use of chits; accounting for keys and key rings; notification of failure to return keys; reporting of broken or lost keys; and the responsible management of the key board/cabinet.

Observation:

Recommendation:

04.02.06 Sound security practices are observed in the consistent, responsible use of interlock systems, sallyports, communication equipment, door locking systems, security gates, etc. for which the control center is responsible.

Observation:

Recommendation:

04.02.07.1 Care is exercised to ensure accurate identification of staff or inmates before access or exit is permitted through controlled doorways and gates.

Observation:

Recommendation:

04.02.08 The control center is securely constructed and has a secure entrance vestibule with interlock doors or a keying system that ensures one of the doors is locked at all times. The entrance is not accessible to inmates. Walls are of reinforced concrete, with security glass and bars. There is not a false ceiling.

Observation:

Recommendation:

04.02.09 The control center is uncluttered and has sufficient storage space for all equipment. All equipment is properly stored to facilitate access and counting. Sight lines to gates, doors, and persons provide clear line-of-sight and ability to operate in a safe and secure manner.

Observation:

Recommendation:

04.02.10 All equipment is serviceable and functioning properly including video monitors, intercoms, fire alarms, electronic locking systems including indicator lights, and perimeter detection system alarm indicators.

Observation:

Recommendation:

04.02.11 Should the control room officer become incapacitated, emergency keys are accessible and stored in a secure area.

Observation:

Recommendation:

05. CONTROLLED MOVEMENT

Objective: *To ensure accountability for all inmates and the safety and security of staff, inmates, and visitors.*

Points of Review:

05.01 Responsibility

05.01.01 There is written policy/procedure that requires control of inmate movement sufficient to ascertain quickly and accurately the location of all assigned inmates at any time. This may be accomplished by several means to include a pass system, gate passes, ID card systems, biometrics, or computer tracking systems.

Observation:

Recommendation:

05.01.02 All movement of individuals or groups of inmates is monitored, tracked, and coordinated with security operations. Written procedure establishes a system for monitoring, tracking, and coordinating the mass movement of inmates (observe movement).

Observation:

Recommendation:

05.01.03 Inmates do not have access to movement documents, including passes, tickets, or the documentation pertaining to any such item.

Observation:

Recommendation:

05.01.04 All inmate movement documents (passes) are legible and bear the authorized signature of a staff member, and include the following information:

- Inmate name and assigned number
- department/area originating the pass
- name and signature of staff originating the pass
- time and date of the pass
- destination
- time of arrival
- signature of receiving staff

Observation:

Recommendation:

- 05.01.05 There is an identification system for inmates assigned to work crews, preferably laminated or embossed work crew cards, which includes the following:
- photo identification; name and number
 - custody level
- If the inmate is on an outside institution work crew the following additional information is included:
- date of birth
 - sentence information

Observation:

Recommendation:

05.02 *Operations*

- 05.02.01 All movement systems have a safeguard system to ensure inmates arrive at their destination. The system includes:
- communication by which staff are alerted that a specified inmate(s) is to be in their area at a specified time;
 - predetermined time-frames within which movement must occur and beyond which the movement time is excessive;
 - written procedure specifying reporting actions to be taken if inmate(s) do not arrive within the specified time; and
 - written procedures specifying actions to be taken to determine an inmate's whereabouts if he/she does not report to the assigned area. .

Observation:

Recommendation:

06. USE OF FORCE

Objective: *To provide direction in the use of force and security equipment to prevent injury to staff, inmates, and others; prevent the destruction of property; and minimize the risk to the general public associated with the escape of inmate(s).*

Points of Review:

06.01 Responsibility

06.01.01 Written policy establishes use of force procedures, specific definition of terms, standardization of equipment, training and documentation requirements, and supervisory protocol.

Observation:

Recommendation:

06.01.02 Written policy requires that only the minimum amount of force necessary to control the situation be used when use of physical force to achieve a legitimate correctional objective is necessary.

Observation:

Recommendation:

06.01.03 Written policy requires all staff involved in a use of force incident to submit reports and supporting documentation.

Observation:

Recommendation:

06.01.04 Written policy requires the examination of the inmate by medical staff immediately after a use of force incident and that the results of the examination be documented.

Observation:

Recommendation:

06.01.05 Written policy states that the use of force as punishment is strictly prohibited.

Observation:

Recommendation:

- 06.01.06 Written policy requires that inmates not be placed in restraints unless it is apparent that to leave the inmate unrestrained would create potential for:
- serious health hazard or injury to inmate or others;
 - escalation of the incident to a serious disturbance;
 - serious destruction of property;
 - loss of control since no other form of control would be effective.

Observation:

Recommendation:

- 06.01.07 Written policy provides protocol for the authorization of the use of chemical agents and provides maximum volume of use for all enclosed areas in which chemical agents could be required.

Observation:

Recommendation:

- 06.01.08 Written policy establishes specific criteria for the use of electronic control devices.

Observation:

Recommendation:

06.02 Training

- 06.02.01 Management, supervisory, operations, and medical staff responsible for use of force related duties are trained consistent with department requirements. Training is adequate to ensure informed and appropriate use of force and includes safeguards to prevent transmission of communicable disease.

Observation:

Recommendation:

06.03 Operations

- 06.03.01 All planned use of force incidents are videotaped. Those uses of force not planned are videotaped from the point that an uninvolved staff member can retrieve a video camera for this purpose.

Observation:

Recommendation:

06.03.02 A multi-tiered (first line, administrative head, executive, etc.) administrative review is required of all incidents in which force is used.

Observation:

Recommendation:

06.03.03 All planned use of force incidents are directed by a shift commander or immediate supervisor.

Observation:

Recommendation:

06.03.04 The wearing of specified protective gear and adherence to sanitation procedures is required in all planned use of force to prevent injury or the transmission of disease. Post-incident medical examinations are required whenever conditions suggest their necessity.

Observation:

Recommendation:

06.03.05 The use of security restraints is terminated after no more than four hours when the inmate has not engaged in behaviors that create potential for:

- serious health hazard or injury to inmate or others;
- escalation of the incident to a serious disturbance;
- serious destruction of property;
- loss of control since no other form of control would be effective.

Observation:

Recommendation:

06.03.06 Inmates controlled with restraints are monitored by security staff and checked by medical staff at intervals required by written policy. Documentation is required.

Observation:

Recommendation:

06.03.07 Electronic devices are not used in conjunction with alcohol based chemical agents or in areas where oxygen-generating equipment is being used.

Observation:

Recommendation:

7. HAZARDOUS MATERIALS MANAGEMENT

Objective: *To provide an environment free of caustic or toxic materials and hazards and ensure that inmates do not have access to materials, which could be used in a harmful or destructive manner.*

Points of Review:

7.01 Responsibility

7.01.01 Written policy requires compliance with all federal, state, and local regulations governing the handling, management, and disposal of hazardous materials.

Observation:

Recommendation:

7.01.02 A perpetual inventory is maintained of all hazardous materials in each department within the facility. Inventories are maintained at the point of storage.

Observation:

Recommendation:

7.02 Operations

10.02.01 Hazardous materials are drawn and issued only by an employee authorized by the warden/superintendent or higher authority.

Observation:

Recommendation:

7.02.02 Inmates are issued chemicals, cleaning agents, caustics etc. in the quantity required to accomplish an immediate task. Unused chemicals are not allowed in work areas at the end of the workday and are inventoried and secured before inmates leave the area.

Observation:

Recommendation:

7.02.03 All hazardous materials issued to inmates or drawn by staff from a point of supply and put in canisters or dispensers are labeled to identify the contents.

Observation:

Recommendation:

7.02.04 Use of all hazardous materials is consistent with the provisions and precautions listed in the Material Safety Data Sheet.

Observation:

Recommendation:

7.02.05 Material Safety Data Sheets are maintained and available for each hazardous substance wherever hazardous substances are stored/used.

Observation:

Recommendation:

7.02.06 All hazardous materials related to hobby craft items are inventoried and controlled by staff and dispensed to inmates only on an as needed basis and under supervision.

Observation:

Recommendation:

7.02.07 All flammable products are managed and controlled as hazardous material and are stored in flammable materials locker in accordance with state and local fire code.

Observation:

Recommendation:

7.02.08 All staff are trained and understand safety/material safety data sheets, and the handling, storage, inventory, and disposal of hazardous materials.

Observation:

Recommendation:

7.02.09 Each department with the potential to handle hazardous materials has clearly labeled hazardous material storage containers in the area.

Observation:

Recommendation:

7.02.10 Disposal of hazardous chemicals is performed in a manner consistent with Occupational Health and Safety Codes. Inmate involvement is not permitted in this activity or, alternatively, is allowed only under continuous direct staff supervision.

Observation:

Recommendation:

7.02.11 Sharps containers are strategically located in areas of use for the storage and/or disposal of sharps and contraband sharps requiring secure safe storage.

Observation:

Recommendation:

8. INMATE MAIL

Objective: *To ensure that the institution mail room operations are consistent with U.S. Postal Regulations and Department policy, and provide adequate safeguards for mail being delivered to staff and inmates.*

Points of Review:

8.01 Responsibility

8.01.01 There is written policy governing the handling of inmate mail including mail and package receipt, inspection, and delivery; legal mail; authorization and documentation of the reading of mail (if required); receipt and handling of money; and the authorization, procedures, and documentation for denial of prohibited types of mail.

Observation:

Recommendation:

8.01.02 There are trained staff assigned responsibility for the daily management of inmate mail.

Observation:

Recommendation:

8.02 Handling and Distribution

8.02.01 Incoming staff mail for distribution within the secure perimeter is inspected before distribution. For sensitive mail it may be inspected in the presence of a representative of the department for which it is intended.

Observation:

Recommendation:

8.02.02 All inmate mail meeting the department criteria for handling as "legal" mail, is opened and inspected in the presence of the inmate to whom addressed.

Observation:

Recommendation:

8.02.03 All mail is under staff control until it is distributed. Inmate workers are not allowed in the mailroom.

Observation:

Recommendation:

8.02.04 All incoming and outgoing inmate mail is inspected for contraband.

Observation:

Recommendation:

8.02.05 All mail received for inmates no longer at the facility is forwarded within three working days.

Observation:

Recommendation:

8.02.06 At institutions of higher custody, detailed inspections (to include fluoroscopic if available), are conducted of all packages (staff and inmate) coming into the mail room to identify contraband that otherwise might go undetected or that might require disassembly of the item to otherwise conduct a thorough search.

Observation:

Recommendation:

8.02.07 Incoming inmate packages are not opened in the inmate's presence unless there is a barrier or screen between the inmate and the staff member opening the package.

Observation:

Recommendation:

8.02.08 Mailroom staff are trained and knowledgeable of what to look for in the area of Security Threat Group (STG) materials.

Observation:

Recommendation:

9. INMATE VISITING

Objective: *To prevent the introduction of contraband during visitation, prevent the utilization of the process to effect escape and to maintain a visiting atmosphere that is safe and comfortable for all visitors.*

Points of Review:

9.01 Responsibility:

9.01.01 Written policy provides clear regulations concerning visitor approval, searches, time and length of visits, number of visitors allowed, personal property visitors may have including medications, visitor and inmate dress, inmate personal property allowed at the visit, physical contact between visitors and inmates, and other factors pertaining to the maintenance of a secure, comfortable, and safe visiting environment.

Observation:

Recommendation:

9.01.02 Written visiting regulations are posted and available for distribution to inmates and visitors.

Observation:

Recommendation:

9.02 Visiting Operations

9.02.01 An approved visitor list is established for each inmate through an application and approval process that includes criminal background checks.

Observation:

Recommendation:

9.02.02 No one is permitted to visit an inmate without advance review and approval.

Observation:

Recommendation:

9.02.03 When a visitor is determined to be on the approved list, he/she must establish his or her identity with a positive picture identification such as a driver's license or the visit is not allowed.

Observation:

Recommendation:

9.02.04 If the visitor cannot provide positive identification, the visit is not allowed.

Observation:

Recommendation:

9.02.05 When approved to visit, and before being permitted into the visiting areas, all visitors are subject to a “hand stamp/black light”, biometric or other equally effective identification procedures to augment picture ID confirmation prior to exit from the facility.

Observation:

Recommendation:

9.02.06 Visitors and their belongings are searched thoroughly before being allowed to pass through the secure perimeter.

Observation:

Recommendation:

9.02.07 Each visitor is required to place all non-essential and otherwise non-allowed personal items in a locker provided by the institution, or to return them to their vehicle. The visitor retains the locker key throughout the visit.

Observation:

Recommendation:

9.02.08 Any items allowed in the visiting room (diaper bags, purses, etc.), are carefully inspected by security staff before the person is allowed into the visiting room.

Observation:

Recommendation:

9.02.09 Each visitor is required to successfully pass through a metal detector: a hand held metal detector is used to search those who activate the alarm in the walk-through unit.

Observation:

Recommendation:

9.02.10 Visitors who repeatedly fail to clear the entrance inspection or refuse to submit to a search are denied the privilege of visiting.

Observation:

Recommendation:

9.02.11 The visitation area is close to the main entrance, has appropriate search and personal item storage areas for visitors, an adequate shakedown area for inmates, separate inmate - visitor restrooms, and a children's play area.

Observation:

Recommendation:

9.02.12 Staff are positioned to provide direct visual supervision of the entire visiting area throughout the visiting period.

Observation:

Recommendation:

9.02.13 Chairs and tables are arranged in a manner that provides direct lines of sight of all visitors and inmates.

Observation:

Recommendation:

9.02.14 Blind spots created by columns, pillars, or other design features are compensated for with mirrors visible from the visiting officers stations. Appropriately placed cameras may be utilized for this purpose as well.

Observation:

Recommendation:

9.02.15 At the completion of visitation all inmates are thoroughly strip searched in an appropriate area designated for that purpose before being allowed to exit the visitation area.

Observation:

Recommendation:

9.02.16 At the conclusion of visitation the visiting area is thoroughly searched and trash disposal outside the facility is either directly supervised or performed by staff.

Observation:

Recommendation:

10. INMATE PROPERTY

Objective: *To control inmate opportunity to acquire, store, transmit, and/or dispose of items of personal property except through authorized channels and to maintain a safe and healthy institution environment.*

Points of Review:

10.01 Responsibility:

10.01.01 There is written policy establishing limitations on the amount of property an inmate may have in his/her possession, a listing of allowable items, and procedures for managing inmate property.

Observation:

Recommendation:

10.01.02 There is an inmate handbook or other written information provided to each inmate that provides complete information about allowable property and the management of inmate property.

Observation:

Recommendation:

10.01.03 Written policy places a maximum dollar value on single items of personal property (e.g. \$100). Major items such as television (if allowed), approved prosthesis, etc. may be exceptions to the limit.

Observation:

Recommendation:

10.01.04 Written policy establishes a disposal process for removal of inmate property that is not claimed by the inmate or next of kin within one year of an inmate's escape, death, parole or mandatory release.

Observation:

Recommendation:

10.02 Inmate Property Management:

10.02.01 An inmate property file is established and maintained for each inmate containing a complete inventory signed by the inmate and the staff responsible for property management.

Observation:

Recommendation:

10.02.02 An up-to-date, perpetual inventory of each inmate's property is maintained and items added or removed as property is received, sent out, or destroyed.

Observation:

Recommendation:

10.02.03 An inmate property area is maintained for the secure storage of property during periods the inmate is in segregation, special housing, or out of the institution (court etc.) A vault/safe is available for the storage of valuables: watches, rings, identification, etc.

Observation:

Recommendation:

10.02.04 The amount and type of property allowed is strictly controlled by the property officers and all non-allowable items received are mailed out at the inmate's expense.

Observation:

Recommendation:

10.02.05 Electronic equipment meets the standards (type, size, value, etc.) established by the department and is etched with the inmate's name and/or number.

Observation:

Recommendation:

10.02.06 Inmates are required to observe institution sanitation standards and requirements for the storage of personal property to facilitate periodic inspections and cell searches.

Observation:

Recommendation:

10.02.07 All items that are not on the inmate's property inventory or allowable property list are confiscated during cell searches and before the transfer or release of the inmate.

Observation:

Recommendation:

10.02.08 Inmates are authorized to possess legal materials in their housing area that directly pertain to pending or active cases before the courts or paroling authority.

Observation:

Recommendation:

10.02.09 All institution staff who are allowed access to the property room receive on-the-job training and are knowledgeable of and can demonstrate compliance through practice/observation and questioning concerning property room procedures.

Observation:

Recommendation:

10.02.10 Property room access is by restricted key only and limited to only those staff designated in writing by the warden or superintendent.

Observation:

Recommendation:

11. INMATE WORK ASSIGNMENTS

Objective: *To provide opportunity for the development of work skills and reduce inmate idleness in a manner which provides for staff safety and public protection.*

Points of Review:

11.01 General Inmate Work Assignment

11.01.01 All persons accepting responsibility for the supervision of inmate workers, including volunteers or other non-correctional, temporary staff, have received training in the supervision of inmates.

Observation:

Recommendation:

11.01.02 Inmate workers do not have access to confidential or sensitive records concerning other inmates or staff either in hard copy, or by computer access.

Observation:

Recommendation:

11.01.03 Inmate workers authorized to use the telephone as a routine part of their work assignment do not have access to, nor opportunity to solicit individual telephone numbers, addresses, social security numbers, credit card numbers, or any information which could compromise the safety and security of another individual.

Observation:

Recommendation:

11.01.04 Telephone printouts are closely monitored for unauthorized use by inmate workers who are authorized telephone access as a routine part of their work. Such telephones are preferably equipped with monitoring and recording capability.

Observation:

Recommendation:

11.01.05 To eliminate the possibility of the use of staff uniforms or personal clothing to effect escape, inmate workers do not have direct access to staff uniforms or personal clothing at any time. Officer uniforms should be stored and issued from a location external to the institutional perimeter.

Observation:

Recommendation:

11.01.06 Inmate workers are routinely strip or frisk searched when departing their work area or, as the sensitivity of the assignment/area requires.

Observation:

Recommendation:

11.01.07 Inmate workers in correctional industry areas are required to proceed through a metal detector upon completion of a frisk search.

Observation:

Recommendation:

11.02 *Outside Inmate Work Assignment*

11.02.01 The general location of all outside work crews is known in the institution central control at all times.

Observation:

Recommendation:

11.02.02 Staff or contractors supervising outside work crews have a picture ID of each inmate assigned to their supervision with them whenever out of the institution.

Observation:

Recommendation:

11.02.03 All vehicles used to transport inmates to and from work locations are searched before inmates are allowed access.

Observation:

Recommendation:

11.02.04 Outside work crews are monitored for size considering the nature of the work, risk presented by the area, and ability of staff/contractor to provide supervision.

Observation:

Recommendation:

11.02.05 Inmates and staff are provided necessary safety equipment for the assignment.

Observation:

Recommendation:

11.02.06 Staff or contract work supervisors have the ability to communication with the institution at all times (telephone or radio).

Observation:

Recommendation:

11.02.07 Institution supervisory staff randomly "spot check" outside crews, documenting each contact.

Observation:

Recommendation:

11.02.08 All outside work crew officers or contractors have signed post orders or written instructions and guidelines.

Observation:

Recommendation:

11.03 *Inmate Work Assignment (Computers)*

11.03.01 There is written policy requiring a review of any requests to grant inmates use of computers and computer technology as part of their work or study assignment.

Observation:

Recommendation:

11.03.02 Inmates are not permitted to enter, view, update, or manipulate information on information systems except by exemption granted by the agency chief executive officer.

Observation:

Recommendation:

11.03.03 Inmates are not allowed to repair or modify any computer equipment except in an authorized training program or upon exemption granted by the agency chief executive officer.

Observation:

Recommendation:

11.03.04 Inmates do not have access to Internet as part of their work assignment. All computers with modems, faxes and access to Internet are in secured areas with no inmate access.

Observation:

Recommendation:

11.03.05 Only stand-alone personal computer equipment is allowed for inmate work assignments. Under no circumstances are inmates allowed opportunity to interface with any component of the agency's network and information system.

Observation:

Recommendation:

11.03.06 An audit of all inmate computers is conducted at least quarterly by knowledgeable staff to prevent abuse or unauthorized use of the systems.

Observation:

Recommendation:

12. INMATE TRANSPORTATION

Objective: *To ensure the safety of staff, inmates, and the public during the transportation of inmates.*

Points of Review:

12.01 *Responsibility*

12.01.01 There is written policy that establishes procedures for the transportation of inmates of varying custody levels between institutions, to community services, and by other than department or institution staff.

Observation:

Recommendation:

12.01.02 Written policy establishes minimum levels of training that must be provided to security staff assigned transportation responsibilities. Currently assigned transportation staff have received the required training. Only trained staff are permitted to fill temporary vacancies (overtime) for transportation duties.

Observation:

Recommendation:

12.01.03 Written policy prohibits notification of an inmate of the date, time, route, and destination of any trip in advance of the trip and the release of this information to persons not having specific need-to-know.

Observation:

Recommendation:

12.01.04 Written policy requires that the transporting officer have a current photo, copy of the inmate's commitment papers, a brief description of the inmate, and a removal/transfer order signed by the warden/superintendent or designee that authorizes the trip in his possession during the transport.

Observation:

Recommendation:

12.01.05 Written policy clearly specifies the level of security supervision, inmate management procedures, and restraint applications to be used in the transport of inmates of various levels of custody.

Observation:

Recommendation:

12.02 *Transport Preparation*

12.02.01 A "removal/transfer order", signed by the warden/superintendent or designee, or court order is provided for the transportation officer as authorization to prepare for the transport of an inmate.

Observation:

Recommendation:

12.02.02 Medical staff are notified of the planned transport and a file review is conducted to determine if there are medical impediments or if medications must accompany the inmate.

Observation:

Recommendation:

12.02.03 The transportation officer-in-charge is present while a thorough search of each inmate is conducted. Strip searches are thorough and are conducted consistent with policy.

Observation:

Recommendation:

12.02.04 Each inmate is positively identified by a supervising officer before exiting the institution.

Observation:

Recommendation:

12.02.05 The transportation officer conducts a thorough vehicle safety check, searches the vehicle interior, and ensures that it is fully fueled before inmates are brought to the vehicle.

Observation:

Recommendation:

12.03 *Transport Procedures*

12.03.01 Inmates who are being transported are under constant and direct supervision from the time they are searched until they are placed in the transport vehicle.

Observation:

Recommendation:

12.03.02 All restraint equipment is double-locked during transport.

Observation:

Recommendation:

12.03.03 If more than one inmate is transported; all are transported at the level of security/custody required by policy for the inmate in the group who is of highest security/custody level.

Observation:

Recommendation:

12.03.04 Except when medical conditions prohibit, all inmates are required to remain in full restraints during medical examination, treatment, or other community services.

Observation:

Recommendation:

12.03.05 Transporting officers have continuous communication capability with a correctional facility and/or local/state law enforcement officials throughout the duration of the trip.

Observation:

Recommendation:

12.04 *High Security Transports:*

12.04.01 Each high security inmate is restrained before leaving the institution by either:

- Option#1, Waist chain, handcuffs with handcuff cover and leg-irons; or
- Option#2, Waist chains equipped with side-cuffs and leg-irons.

Observation:

Recommendation:

12.04.02 Policy requires that high security inmates be under constant armed supervision when outside the secure perimeter of the institution and observation confirms this requirement is followed.

Observation:

Recommendation:

12.04.03 All high security transport officers are equipped with non-lethal control devices, body armor and agency approved lethal weapons.

Observation:

Recommendation:

12.04.04 During specified high security transports:

- a) A transport vehicle is accompanied by a trailing vehicle escort driven by an officer armed with a lethal weapon, and
- b) Communication between the two vehicles and the base station is maintained throughout the transport.

Observation:

Recommendation:

12.04.05 A minimum of two officers is required in the lead vehicle and one in the trailing vehicle during a high security inmate transport where a trailing vehicle is required.

Observation:

Recommendation:

12.04.06 All vehicles that are used to transport high security inmates are equipped with a vehicle radio, security screens, and external door locks.

Observation:

Recommendation:

12.04.07 All high security inmates are under constant sight and sound supervision during transportation preparation, transport, and during off-loading procedures.

Observation:

Recommendation:

13. KEY CONTROL

Objective: *To provide control and accountability of all keys and locking systems and establish key control procedures that, when properly attended, will afford the protection and security intended in the design of the locking systems.*

Points of Review:

13.01 Responsibility

13.01.01 There is a comprehensive key control policy that is clearly written, maintained in a secure area, and available to staff for reference purposes.

Observation:

Recommendation:

13.01.02 A locksmith or fully trained key control officer is assigned responsibility for key control and maintenance and maintenance of locking devices.

Observation:

Recommendation:

13.01.03 A staff member is assigned to assist the locksmith/key control officer and to provide backup assistance in the absence of the locksmith or during institution emergency.

Observation:

Recommendation:

13.01.04 There are position descriptions and current post orders that describe the duties and responsibilities of the locksmith/key control officer and locksmith/ key control officer assistant.

Observation:

Recommendation:

13.01.05 The post orders of officers who issue keys fully describe the responsibilities related to issuance and retrieval of keys/key rings and reporting loss, breakage, or failure to return keys.

Observation:

Recommendation:

13.01.06 There is written policy and procedure pertaining to the loss, breakage, or failure to return keys, including verbal and written reports, search procedures, immediate inventory and identification, and changing of locks in affected areas.

Observation:

Recommendation:

13.01.07 There is written institution policy prohibiting the handling of security keys by inmates.

Observation:

Recommendation:

13.01.08 A comprehensive audit of the key control program is conducted annually by knowledgeable staff from another institution or a central audit unit.

Observation:

Recommendation:

13.01.09 Training is provided to the locksmith/key control officer and locksmith/key control officer assistant.

Observation:

Recommendation:

13.02 *Records and Documentation*

13.02.01 Key control record systems are restricted and available to staff only on a need-to-know basis.

Observation:

Recommendation:

13.02.02 There is comprehensive documentation of the facility locking system that is sufficient to reconstruct the entire locking system and that provides a history of lock utilization.

Observation:

Recommendation:

13.02.03 A perpetual inventory and cross inventory of all keys, blanks, pattern keys, and locks is maintained. Documentation is current and accurately reflects what is actually on site.

Observation:

Recommendation:

13.02.04 Keys, pattern keys, blanks, and locks are securely stored and inventoried using a systematic filing and storage method that ensures strict accountability.

Observation:

Recommendation:

13.02.05 All cut keys and key blanks are assigned a storage hook number and maintained in a storage cabinet(s) with a copy of the current inventory. A perpetual inventory is maintained.

Observation:

Recommendation:

13.02.06 The number of copies and blanks for any given key in the storage area agrees with the documentation.

Observation:

Recommendation:

13.02.07 Key rings have been soldered or otherwise secured to prevent removal or loss of keys or identifying information.

Observation:

Recommendation:

13.02.08 Written authorization is provided by the facility security chief before any duplication of keys or the modification of a lock or locking system.

Observation:

Recommendation:

13.02.09 Changes in inventory, lock deployment, or key utilization are accompanied by immediate notation in the related records. Perpetual inventories of key blanks and other critical items are updated as items are added or removed from stock.

Observation:

Recommendation:

13.02.10 An internal inventory of the lock shop is conducted at least quarterly by a supervisor other than the locksmith or other person designated by the Warden/Superintendent to be responsible for key control.

Observation:

Recommendation:

13.02.11 The permanent issue of keys is controlled by institution policy and is limited to exceptional circumstances. A quarterly inventory is conducted of all permanent-issue key rings.

Observation:

Recommendation:

13.02.12 A report of each inventory, with all discrepancies and recommendations for improvements and changes, is sent to the facility's head of security.

Observation:

Recommendation:

13.02.13 There is documentation for each key, cross-referenced by the following:

Location, filed alphabetically, indicating:

- The lock for which the key is cut

Lock make, model, manufacturer's number, and brand name:

- Key code number
- Key rings on which the key is included
- Key ring hook number of each ring containing the key
- Emergency key rings containing the key (if any)
- Hook number of the key in the storage cabinet (if used)

Hook number in the storage cabinet, filed numerically, indexed to:

- Location
- Which lock is fitted by the key assigned to this hook number

Lock make and model, including brand name and manufacturer's number, indicating:

- All blanks indexed by manufacturer's number for blank key stock
- Hook number in the storage cabinet

Observation:

Recommendation:

13.03 Issue of Keys

13.03.01 All keys are returned to the issuing location at the end of the workday or when the employee to whom the keys were issued leaves the institution.

Observation:

Recommendation:

13.03.02 A clearly marked, convenient keyboard or cabinet is used for key issue, return, and storage that ensures ease of access, security, and total accountability.

Observation:

Recommendation:

13.04.03 There is special designation on the key board/cabinet for key rings that are issued on a permanent basis, keys that are inactive, and hooks that are not in use.

Observation:

Recommendation:

13.03.04 Keys are issued from a secure control center or similar reinforced area that is not accessible to inmates.

Observation:

Recommendation:

13.03.05 All key sets have a tag indicating the key ring number and a tag indicating the number of keys on the ring.

Observation:

Recommendation:

13.03.06 There is a daily accounting for all keys (key count).

Observation:

Recommendation:

13.03.07 There is system of key “chits” or an issue log for recording and documenting the issue of keys.

Observation:

Recommendation:

13.03.08 No keys are issued or maintained within the institution proper that will allow complete egress from the institution.

Observation:

Recommendation:

13.04 *Emergency Keys*

13.04.01 Emergency key rings for various buildings and areas of the institution are stored in a readily accessible, secure control center.

Observation:

Recommendation:

13.04.02 Emergency keys and locks are color coded for quick identification.

Observation:

Recommendation:

13.04.03 Emergency keys and locks are notched for low light identification.

Observation:

Recommendation:

13.04.04 Emergency key rings have a metal ring disc (“chit”) stamped with the name of the area the ring accesses and the number of keys on the ring.

Observation:

Recommendation:

13.04.05 If emergency key rings are located outside the control center, are there chits on the hooks in the control center cabinet showing the key location.

Observation:

Recommendation:

13.04.06 Emergency keys are stored in a readily accessible place that is clearly separate from the standard key-issue board or cabinet. There is an alphabetical listing or a schematic drawing of the areas served by the various rings, each with the corresponding ring number, prominently posted.

Observation:

Recommendation:

13.04.07 A duplicate emergency keyboard is maintained outside the secure perimeter such as in a tower or armory.

Observation:

Recommendation:

13.04.08 Emergency keys to the perimeter locks and gates are maintained outside the secure perimeter and access is restricted by institution or department policy.

Observation:

Recommendation:

13.04.09 Emergency keys are rotated to equalize wear and all emergency keys/ locks are tested at least quarterly. A ledger including documentation of such checks and the reported deficiencies is maintained on a permanent basis.

Observation:

Recommendation:

13.04.10 The issuing of emergency keys is restricted by policy and is clearly indicated on the emergency key board/cabinet to prevent access to sensitive areas by unauthorized staff.

Observation:

Recommendation:

13.04.11 Emergency keys are included in the daily key count.

Observation:

Recommendation:

13.04.12 A record of the issuance of restricted keys is maintained bearing the key ring number, date, time of issue and return, the person to whom issued, the purpose of the issue, and the person authorizing the issue.

Observation:

Recommendation:

13.04.13 There are greater levels of restricted access maintained over some highly sensitive areas such as pharmacy, armory, lock shop, etc. Such control is maintained by use of glass door compartments or sequentially numbered seals, signature of the issuing officer and person to whom issued, written reports of issue, etc.

Observation:

Recommendation:

13.05 Lock shop

13.05.01 There is a lock shop outside the secure perimeter of the institution with sufficient space for the basic tools necessary for lock repair, the orderly storage of keys, blanks, chits, and other supplies, and maintaining/filing of all records pertaining to the locking system of the institution.

Observation:

Recommendation:

13.05.02 The lock shop is of high-security construction: poured or reinforced concrete blocks with rebar, solid ceiling (not suspended or “false”), without wall openings (window, air conditioner, vents), and, at minimum, a 14 gauge steel door.

Observation:

Recommendation:

13.05.03 There is a sally-port entrance to the lock shop or, if not, other precautions are taken to restrict access to the area.

Observation:

Recommendation:

13.05.04 The lock shop is equipped to facilitate all of the basic key control operations within or, if not, all key/lock related equipment and activities are located in other highly secure areas.

Observation:

Recommendation:

13.05.05 Access to the lock shop is restricted to authorized personnel and a log is maintained of all persons accessing the area.

Observation:

Recommendation:

13.05.06 The filing and storage of keys, pattern keys, blanks, chits, and other keying supplies demonstrates order and systematic, ongoing control of all key control processes.

Observation:

Recommendation:

13.05.07 There is a specific, secure board/cabinet maintained that holds a pattern key and at least one additional key for each lock in the institution.

Observation:

Recommendation:

13.05.08 Pattern keys are easily distinguished from the duplicates.

Observation:

Recommendation:

13.05.09 An up-to-date blueprint of the entire facility is secured in the lock shop that indicates the location and type of all locks.

Observation:

Recommendation:

13.05.10 Worn, broken, or discarded locks are routinely destroyed and records maintained of their destruction.

Observation:

Recommendation:

13.05.11 Procedural safeguards are in place that prevent the delivery of lock shop supplies through the general institution warehouse without proper controls.

Observation:

Recommendation:

14. PERIMETER SECURITY

Objective: *To provide an effective control and security barrier as the last major line of defense against escape and intrusion.*

Points of Review:

14.01 Responsibility

14.01.01 There is written agency policy that designates a security level for the institution and specific perimeter design/construction requirements related to that security level.

Observation:

Recommendation:

14.01.02 There is written institution policy that establishes a requirement and procedures for continuous surveillance of the institution perimeter.

Observation:

Recommendation:

14.01.03 There is an electronic technician on staff and/or on call who is formally trained in the maintenance and repair of all perimeter electronic detection systems and other electronic equipment in use in the institution.

Observation:

Recommendation:

14.02 Perimeter Design and Condition

14.02.01 The inner and outer fence heights are appropriate for the security designation of the institution and consistent with department policy.

Designation _____ Inner Fence Height _____ Outer Fence Height

Observation:

Recommendation:

14.02.02 The number of inner and outer razor rolls and the type of barb used (long or short) is appropriate for the perimeter security category of the institution being reviewed.

Observation:

Recommendation:

14.02.03 The inner and outer concrete slabs/aprons at the fence base are appropriate for the perimeter security category of the institution being reviewed.

Observation:

Recommendation:

14.02.04 Perimeter lighting between the fences and thirty (30) feet on either side provides low-light vision and complies with department standards.

Observation:

Recommendation:

14.02.05 Perimeter lighting is connected to a reliable emergency power supply and tested at least monthly.

Observation:

Recommendation:

14.02.06 There are no rusted or broken areas on the perimeter fence or accompanying barrier wires that compromise the integrity of the perimeter.

Observation:

Recommendation:

14.02.07 There are no washed out areas or gaps greater than two (2) inches at the bottom of the perimeter fence or under concrete pads.

Observation:

Recommendation:

14.02.08 Drainage pipes under the perimeter fence are no larger than 10 inches in diameter or are secured/closed with steel grating. Drainage outfalls are secured with a headwall or bar gate.

Observation:

Recommendation:

14.02.09 All landscaping trees and vegetation which could provide cover, obstruct line of observation, or otherwise be used to facilitate escape have been removed from within seventy feet of the inner perimeter fence, between the fences and adjacent to the outer fence.

Observation:

Recommendation:

14.02.10 All perimeter towers and rover vehicles are equipped with hand operated spotlights and communication equipment.

Observation:

Recommendation:

14.02.11 Inner compound cross fencing that intersects with the perimeter fence incorporates razor wire on both sides along the top for a least a 10 foot span on the intersecting fence.

Observation:

Recommendation:

14.02.12 An inner and outer crash barrier system is installed at every breach in the perimeter fence created for the purpose of vehicular access to the institution.

Observation:

Recommendation:

14.02.13 Trash compactors/dumpsters are secured with a hasp and lock.

Observation:

Recommendation:

14.03 *Electronic Detection Systems*

14.03.01 The type of electronic detection system is appropriate for the perimeter security designation of the institution, weather conditions, soil conditions, and landscape.

Observation:

Recommendation:

14.03.02 The alarm zones for perimeter electronic detection systems are clearly marked on the outer fence and are visible from the perimeter road.

Observation:

Recommendation:

14.03.03 Perimeter electronic detection systems tie into all inner compound cross fencing for the distance of at least one full fence panel.

Observation:

Recommendation:

14.03.04 Each zone of an electronic detection system is checked every 24 hours and a report of the findings is forwarded to the institution security chief.

Observation:

Recommendation:

14.04 Perimeter Surveillance and Control

14.04.01 Perimeter patrol vehicles are maintained in a safe and fully operable condition.

Observation:

Recommendation:

14.04.02 A security supervisor makes an unannounced daily visit to each perimeter post at least once during the shift.

Observation:

Recommendation:

14.04.03 Perimeter staff are knowledgeable of appropriate actions when confronting suspicious persons or situations.

Observation:

Recommendation:

14.04.04 Perimeter staff are knowledgeable of appropriate actions in response to helicopter or aircraft intrusion.

Observation:

Recommendation:

14.04.05 Perimeter staff are knowledgeable of appropriate actions in response to escape attempts.

Observation:

Recommendation:

14.04.06 Perimeter staff demonstrate competence in use of weapons and use of force policy including a clear understanding of the point at which it is permissible to use deadly force on an inmate attempting to escape.

Observation:

Recommendation:

14.04.07 Perimeter staff are knowledgeable of appropriate actions in response to hostage situations.

Observation:

Recommendation:

14.04.08 Perimeter staff demonstrate competence in relief procedures, equipment exchange, and response time to specific areas of the perimeter.

Observation:

Recommendation:

14.04.09 Security procedures prevent inmate access to buildings located on the perimeter that are points of facility entrance and egress.

Observation:

Recommendation:

14.05 *Access and Egress: Staff, Visitor, and Inmate*

14.05.01 Employees with inner-institution assignments and all visitors are processed through the main entrance of the institution.

Observation:

Recommendation:

14.05.02 The identification of all persons entering and exiting the institution is determined and verified by staff assigned and trained to control access and egress.

Observation:

Recommendation:

14.05.03 All permanent staff present a picture identification card; occasional visitors and workers are provided temporary identification cards. Control staff visually verify that the bearer of the card is the person authorized to enter/exit.

Observation:

Recommendation:

14.05.04 A log of non-employees who are permitted to enter the facility is maintained and reviewed by a control room supervisor at the beginning of each shift. Positive identification is made before entry and exit from the facility is granted.

Observation:

Recommendation:

14.05.05 All inmates exiting the institution are searched upon entry or exit, identified by photograph, logged out, and their identity verified upon return.

Observation:

Recommendation:

14.05.06 Inmates are not allowed to carry articles out of or into the institution.

Observation:

Recommendation:

14.05.07 All purses, packages, toolboxes, etc. are inspected before being allowed in the institution.

Observation:

Recommendation:

14.05.08 There is a written policy and procedure governing inmate admission and discharge processes, including procedures specifically addressing the admission and release of inmates of high profile in the community.

Observation:

Recommendation:

14.05.09 Identification processes are initiated upon admission including fingerprinting, photo, review of personal identification, and verification with attendant commitment documents.

Observation:

Recommendation:

14.05.10 During the admission process inmates are strip searched and housed separately from others until precautions are taken to prevent contagion.

Observation:

Recommendation:

14.05.11 Inmates are positively identified (picture I.D.) and the release documentation reviewed at the point of release by a supervising security staff member.

Observation:

Recommendation:

14.06 Access and Egress: Vehicles and Equipment

14.06.01 All vehicles, trailers, carts, equipment, etc. are thoroughly inspected before being allowed to enter or exit the institution.

Observation:

Recommendation:

14.06.02 Trucks that are loaded or unloaded within the institution are kept under the supervision of an employee or escort officer. Loaded vehicles are allowed to leave the facility only after the clearing of count.

Observation:

Recommendation:

14.06.03 All commercial vehicles are accompanied by an assigned escort officer while in the institution.

Observation:

Recommendation:

14.06.04 Steering wheel locks are used in all vehicles entering the institution or vehicles are locked in a secure area under supervision of staff.

Observation:

Recommendation:

14.06.05 Vehicles and equipment remaining in the institution overnight are rendered inoperable by removal of an engine part necessary to their operation.

Observation:

Recommendation:

14.06.06 No vehicles other than authorized emergency vehicles are allowed to enter or exit the institution during a period of count.

Observation:

Recommendation:

14.06.07 Perimeter sally port gates are operated as an interlocked system. Overrides are approved and supervised by a ranking security officer.

Observation:

Recommendation:

14.06.08 All perimeter sally port gates are operated from a secure location remote from the inmate and the vehicular traffic.

Observation:

Recommendation:

14.06.09 Perimeter vehicle gates are designed to accommodate all emergency vehicles including ladder trucks, and other over-sized emergency vehicles.

Observation:

Recommendation:

15. PHYSICAL PLANT

Objective: *To provide housing, activity, operations, and support space that is suitable to the needs of the inmate population and staffing structure and provides for the safety and security of staff, inmates, and the community.*

Points of Review:

15.01 *Design and Construction:*

15.01.01 In construction, renovation, and arrangement of work areas, good visibility has been maintained to ensure an optimal level of visual supervision.

Observation:

Recommendation:

15.01.02 Building additions/attachments, awnings, light posts, etc. do not provide access to rooftops or create blind spots that compromise visual supervision.

Observation:

Recommendation:

15.01.03 All high security work areas have a primary and alternate evacuation route for staff and inmates in emergency conditions.

Observation:

Recommendation:

15.01.04 Security hardware (doors, window and door frames, glazing, locking devices, and control systems) are appropriate to the institution's security designation and consistent with agency standards.

Observation:

Recommendation:

15.01.05 Control Centers (ceiling, walls, floor etc.) are constructed of rebar reinforced concrete with at least 2 hr. security glass and bars.

Observation:

Recommendation:

15.01.06 Materials, fixture type, and placement or installation (sinks, toilets, towel racks, lights, ceiling/wall material, bed frames, clothing hooks, etc.) are consistent with the institution's security designation, agency standards, and do not present health, safety, or security problems.

Observation:

Recommendation:

15.02 Operations and Maintenance

15.02.01 Institution landscaping does not obscure line of sight for towers, mobile patrol, or other essential posts, or otherwise compromise security.

Observation:

Recommendation:

15.02.02 Items and equipment that may afford hiding for an inmate, or may be used to scale a fence or wall are secured and are a safe distance from the fence/wall.

Observation:

Recommendation:

15.02.03 Areas in which inmates work or reside do not have objects, equipment etc. stacked in work areas or wall dividers (temporary or permanent) that interfere with visual observation. The storage of goods and equipment is limited to that immediately necessary and is securely stored against outside walls.

Observation:

Recommendation:

15.02.04 Rooftops are unobstructed and, where buildings adjoin a perimeter fence or wall, precautions are taken to ensure that inmates cannot access the fence/wall from the rooftop.

Observation:

Recommendation:

15.02.05 All security system related power/technology equipment is inspected for proper operation and is routinely maintained. Maintenance documentation is available.

Observation:

Recommendation:

15.02.06 Staff are trained in the operation of new security equipment and technology and their proficiency is tested on a random basis by supervisors.

Observation:

Recommendation:

15.02.07 Security systems (emergency doors, duress alarms, communications, fire suppression systems, etc.) are tested on a regular basis with documentation of testing outcomes.

Observation:

Recommendation:

15.02.08 Emergency generators provide 100% power back-up to critical security systems (lighting, security door operations, etc.) and instantaneous, 100% battery based uninterrupted power supply (UPS) to critical security functions such as communications, alarm reporting, and computer systems.

Observation:

Recommendation:

15.02.09 Emergency generators are located in a secure area and tested weekly. "Start-up" and full load tests are conducted once each quarter. Maintenance activity and testing outcomes are documented. UPS power back up is tested at least monthly.

Observation:

Recommendation:

15.02.10 Emergency generators have a minimum 72-hour fuel supply and a locking fuel cap.

Observation:

Recommendation:

15.02.11 All administrative staff and supervisors have knowledge of which systems the emergency generator will operate in event of an emergency.

Observation:

Recommendation:

15.03 *Construction Sites*

15.03.01 There is written policy or procedure governing the supervision of construction within and adjacent to the secure perimeter, including security clearance of construction workers, vehicle access, tool inventory and control, supplies and equipment, hours of work, and supervision of worker and vehicle or equipment movement.

Observation:

Recommendation:

15.03.02 Secure fencing is installed around major construction areas within the secure perimeter of the institution within which all vehicles, equipment, and supplies are secured.

Observation:

Recommendation:

15.03.03 Any planned interruption of utility services or stoppage of inmate movement or program is communicated to the chief of security no less than 48 hours before its occurrence.

Observation:

Recommendation:

15.03.04 Accommodation is made to ensure safety and security when construction activity creates a hazard of any nature including reduced surveillance from towers or other officer posts.

Observation:

Recommendation:

16. POST ORDERS

Objective: *To establish guidelines for the development, revision, implementation, and monitoring of post-specific security procedures and requirements.*

Points of Review:

16.01 Responsibility:

16.01.01 Written policy establishes a requirement that post orders be current, complete, and available at each security post.

Observation:

Recommendation:

16.01.02 The facility's chief security officer has established a system to ensure that post orders are reviewed and signed by the assigned officer, relief staff, and others rotating through the post on each shift.

Observation:

Recommendation:

16.01.03 There is written policy governing the interim amendment of post orders and the ongoing review and annual revision of all post orders. Each "retired" post order is archived for a minimum of three years for reference in legal challenges.

Observation:

Recommendation:

16.02 Post Order Content

16.02.01 All post orders contain general instructions similar to the following, and others deemed important by the warden/superintendent:
"Any employee taken hostage, or otherwise under duress is without any authority, regardless of rank."
"Post orders cannot cover every incident or eventuality. Employees assigned to any post shall use good judgment and pay careful attention to the general and specific issues and details related to the post of assignment."

Observation:

Recommendation:

16.02.02 Post orders provide specific information concerning the expectations and requirements related to the post assignment and include the following major categories, as applicable:

- Zone of Control
- Inventory Control
- Key Control
- Use of Force (including helicopter escape)
- Traffic Control
- Count Procedures
- Escort Procedures
- Relief Procedures
- Incident Reporting
- Record Keeping
- Scheduled Activities
- Emergency Procedures for that Area
- Hazardous Material Control
- Maintenance/Repair Requests

Observations:

Recommendations:

16.02.03 There are current post orders for temporary or emergency posts, including the following:

Tactical Team	Attempted Suicide
Crime Scene Preservation	Dry Cell
Escape	Evacuations
Hospital Watch	

Note: Some temporary/emergency post orders (hospital watch, dry cell, crime scene preservation, attempted suicide, etc.) may be in with general post orders; however others such as escape, tactical team, evacuations, etc. that are of a highly sensitive nature should be maintained in confidential manuals in secure areas so inmates **never gain access to compromising documentation.**

Observation:

Recommendation:

16.02.04 Highly sensitive post orders such as those for emergency response teams and tactical teams are maintained in manuals stored in secure areas and marked confidential.

Observation:

Recommendation:

17. SEARCHES

Objective: *To provide surveillance of inmates, staff, and visitors and all areas of the institution to ensure a safe and healthful environment that is free of dangerous weapons and other contraband, clutter that creates fire or other hazard, and responsible management of institution resources including linens, foodstuffs, cleaning supplies, etc.*

Points of Review:

17.01 Responsibility

17.01.01 Written policy establishes responsibility for a system of searches and procedures for the search of all areas of the institution; staff; visitors; inmates; vehicles; mail; inmate property; warehouse goods; and other persons or activities that may pose a threat through the introduction of contraband into the institution.

Observation:

Recommendation:

17.01.02 Written policy establishes requirements for the documentation of all searches to ensure that all areas of the institution are inspected within a reasonable time frame and to ensure the integrity of the search program.

Observation:

Recommendation:

17.01.03 All officer staff have received training in the conducting of cell and area searches, frisk and strip searches, and authorized searches of visitors, guests, and staff in a manner that ensures the detection of all contraband.

Observation:

Recommendation:

17.02 Cell Searches

17.02.01 Post Orders require the search of all inmate cells/rooms at least monthly.

Observation:

Recommendation:

17.02.02 All cell/room searches are documented and logged in an official search log with notation of the search date, cell searched, and contraband discovered.

Observation:

Recommendation:

17.02.03 Cells/rooms are left in a reasonably neat and orderly condition by the officer conducting the search. Care is taken to ensure authorized property is not damaged or disposed of.

Observation:

Recommendation:

17.02.04 The inmate whose cell/room is being searched or a second officer, is present during a cell/room search whenever possible.

Observation:

Recommendation:

17.02.05 Equipment such as flashlights, gloves and mirrors are made available to officers conducting cell searches.

Observation:

Recommendation:

17.02.06 The cell being searched is secured if the staff conducting the search are required to leave the cell prior to completion of search. The search is completed as soon as possible and always within 2 hours.

Observation:

Recommendation:

17.02.07 Each vacated cell is searched thoroughly before occupancy by another inmate to remove contraband and document damage to the cell interior and furnishings. Preferably the inmate occupying the cells signs a form accepting responsibility for the cell with any noted deficiencies.

Observation:

Recommendation:

17.02.08 Cells used for suicide watch are thoroughly searched before use and all non-secured items are removed.

Observation:

Recommendation:

17.03 Area Searches

17.03.01 Searches of common areas are conducted on a regular (once a week) unannounced basis. Areas that are routinely searched include culinary, vocational, education, dayroom, recreation, visiting areas, industry shops, and other areas to which inmates may have access.

Observation:

Recommendation:

17.03.02 Area searches are documented on an official search log. The log notes the search date, area searched, and contraband discovered.

Observation:

Recommendation:

17.04 Frisk (Pat) Searches

17.04.01 Frisk searches are systematic, thorough searches that are consistent with training standards. All items on the inmate's person are searched.

Observation:

Recommendation:

17.04.02 Random and routine frisk searches are conducted on inmates in all areas of the institution and off institution grounds.

Observation:

Recommendation:

17.05 Strip Searches

17.05.01 Routine strip searches are conducted by an officer of the same sex as the inmate in a place and manner that affords a degree of privacy. Emergency strip searches are conducted in an area that affords privacy if conditions allow. Emergency strip searches are conducted by officers of the same sex unless no other reasonable/feasible alternative exists.

Observation:

Recommendation:

17.05.02 Strip searches are systematic, thorough, and consistent with training standards. Inmates are not touched during the search unless the inmate is violent and behavior warrants physical intervention.

Observation:

Recommendation:

22.05.03 Documentation is maintained of all strip searches.

Observation:

Recommendation:

17.06 Body Cavity Searches

17.06.01 Written policy establishes specific conditions for authorization and specific procedures for conducting a body cavity search.

Observation:

Recommendation:

17.06.02 Body cavity searches are conducted only by medical staff.

Observation:

Recommendation:

17.06.03 Thorough documentation is maintained of probable cause for search, the authorizing official, and the findings of the search.

Observation:

Recommendation:

17.07 *Disposition of Contraband*

17.07.01 An inmate found in possession of contraband is issued a receipt for its removal unless the item is clearly determined to be state property. The receipt may be in the form of a violation report.

Observation:

Recommendation:

17.07.02 A secure storage area is designated for contraband storage during referral of a contraband charge to disciplinary proceedings or outside court.

Observation:

Recommendation:

017.07.03 An inmate is permitted to exercise options for disposition of property (send home, destroy, donate to state, etc.) if the contraband was legitimately acquired, ownership is established, and it does not create danger to handlers.

Observation:

Recommendation:

17.07.04 Inmates are notified of the maximum period of time contraband may be held before disposition.

Observation:

Recommendation:

17.07.05 All inmate appeals or court actions are exhausted before disposition of contraband.

Observation:

Recommendation:

17.07.06 Inmate property records are reconciled following any transaction (purchase, receipt, transfer, destruction of property).

Observation:

Recommendation:

17.07.07 Record of disposition and witnesses to the disposition are maintained. Disposition methods cannot personally benefit staff.

Observation:

Recommendation:

17.08 Chain of Evidence

17.08.01 The warden/superintendent has assigned responsibility for evidence management to one staff member.

Observation:

Recommendation:

17.08.02 A secure storage area is designated for evidence storage that is accessible to authorized staff only.

Observation:

Recommendation:

17.08.03 All evidence is assigned a number and logged in the secure storage area by the Shift Commander. The logging information is securely attached to the evidence or container containing the evidence.

Observation:

Recommendation:

17.08.04 Separate storage in the secure storage area is provided for evidence that is dangerous in nature, was used in commission of a crime, or is potentially relevant in a felony prosecution.

Observation:

Recommendation:

17.08.05 Access to the evidence storage area is limited to authorized personnel and all access and egress is logged by person, date, and evidence number.

Observation:

Recommendation:

17.08.06 Disposition of evidence is logged, the log including at minimum, the name, date, method of disposition, and witness(s) to the disposition.

Observation:

Recommendation:

18. SECURITY INSPECTIONS

Objective: *To ensure the integrity of buildings, perimeter enclosures, equipment, utilities, and grounds as related to institution security and safety.*

Points of Review:

18.01 Responsibility

18.01.01 There is written policy that requires systematic inspection of all equipment and areas of the institution and procedures to ensure compliance with policy and documentation of inspection activities.

Observation:

Recommendation:

18.01.02 Staff assigned to conduct security inspections complete a written report of each area inspected noting the weaknesses or deficiencies of each.

Observation:

Recommendation:

18.01.03 Each security inspection report is reviewed by the institution security chief and action taken as appropriate to the needs identified. Inspection reports are maintained at least 30 days.

Observation:

Recommendation:

18.02 Security Inspection Requirements

18.02.01 All perimeter fences, buildings, walls, windows, doors, and drainage pipes (over 10 inches wide with steel grating), which are on or adjoin the perimeter, are inspected at least once each day: in the evening shift before dark. Completion of the perimeter inspection is logged.

Observation:

Recommendation:

18.02.02 Each zone of an electronic perimeter detection system is tested daily in a manner consistent with the manufacturers specifications.

Observation:

Recommendation:

18.02.03 Fences (including interior compound fences) are inspected at least weekly.

Observation:

Recommendation:

18.02.04 All control room doors and windows are inspected daily to ensure security.

Observation:

Recommendation:

18.02.05 Control room windows are uncluttered to permit clear viewing of all areas.

Observation:

Recommendation:

18.02.6 The control room pass-through is not used as talk-through and is not routinely open.

Observation:

Recommendation:

18.02.07 Emergency exit doors and keys are checked weekly to ensure they are in operating order. The physical check is logged.

Observation:

Recommendation:

18.02.08 The exterior windows of all housing areas are inspected daily. All inmate housing area windows and cell bars are physically challenged by staff through pounding with a rubber mallet at least twice weekly. Documentation is maintained.

Observation:

Recommendation:

18.02.09 All towers are inspected at least weekly.

Observation:

Recommendation:

18.02.10 The grounds, including shrubbery and landscape, are inspected at least weekly.

Observation:

Recommendation:

18.02.11 The buildings outside the facility perimeter are inspected at least weekly.

Observation:

Recommendation:

18.02.11 All interior buildings are examined for evidence of tunneling at least once a month.

Observation:

Recommendation:

18.02.12 Maintenance tunnels are inspected at least once a week

Observation:

Recommendation:

18.02.13 The visitor parking area is inspected daily, before and after visitation.

Observation:

Recommendation:

18.02.14 A systematic approach is used to address security weaknesses and deficiencies that are identified and corrective actions are taken within reasonable time frames.

Observation:

Recommendation:

19. SEGREGATION (SPECIAL MANAGEMENT)

Objective: *To provide for the humane and secure control of disruptive inmates, and ensure a safe environment for staff and inmates.*

Points of Review:

19.01 Responsibility

19.01.01 Written policy establishes responsibility for the operation of segregated housing areas that may include disciplinary segregation, administrative confinement, protective custody, and special program units.

Observation:

Recommendation:

19.01.02 Written policy clearly states criteria and procedures for placement and release from segregated housing areas, conditions of confinement, program components of the placement that pertain to eligibility for release, and review procedures.

Observation:

Recommendation:

19.01.03 Written policy establishes a requirement that the security chief, assistant warden/superintendent(s), and warden/superintendent visit special housing units at least weekly. Sign-in logs document their visitation on a regular basis.

Observation:

Recommendation:

19.01.04 Written policy establishes procedures for routine and special review of inmate program, mental health, health, and housing needs, progress toward release, and sanctions.

Observation:

Recommendation:

19.02 Staffing

19.02.01 Staff assigned to disciplinary or administrative segregation units are trained in the management of violent and disruptive inmates, cell extraction procedures, and use of force policy.

Observation:

Recommendation:

19.02.02 Staff assigned to disciplinary or administrative segregation units are experienced in security and inmate management. Probationary staff are prohibited from occupying a post in these units.

Observation:

Recommendation:

19.02.03 Regularly assigned staff are rotated from segregated housing units at intervals specified by department policy (preferably not in excess of two years).

Observation:

Recommendation:

19.02.04 Sign-in logs establish that Medical staff visit the unit daily and that inmates are advised of their presence and availability if needed.

Observation:

Recommendation:

19.02.05 Sign-in logs establish that the officer-in-charge of each shift visits each segregated housing unit at least once during his/her shift.

Observation:

Recommendation:

19.03 Segregation Operations

19.03.01 Protective Custody inmates are housed separately from known enemies and from inmates in disciplinary segregation.

Observation:

Recommendation:

19.03.02 Staff observation checks of inmates in segregated housing areas are conducted at least every 30 minutes. Documentation demonstrates that such checks occur.

Observation:

Recommendation:

19.03.03 A thorough cell search is conducted each time an inmate is removed for a shower, exercise, or for other purposes.

Observation:

Recommendation:

19.03.04 Documentation for each inmate includes, at minimum, the following information: movement in and out; visitors to the unit; cell assignments; unusual incidents; cell searches; inmate telephone calls; 30 minute checks; all meals, services, and activities not provided an inmate as required and the reason; refusals to eat, etc.; exercise periods; and showers.

Observation:

Recommendation:

19.03.05 Only one inmate is allowed out-of-cell in an individual secure area at any one time.

Observation:

Recommendation:

19.03.06 A ratio of two staff to one inmate is required whenever an inmate is removed from his/her cell in the segregated housing unit. Once a strip search has been conducted and the restraints applied and carefully checked, one officer may complete the escort while inside the secure segregation area.

Observation:

Recommendation:

19.03.07 Each inmate is placed in handcuffs before the cell door is opened. Additionally waist chains and leg shackles are required for any escort outside the secure segregation area.

Observation:

Recommendation:

19.03.08 Inmates are thoroughly strip searched before entering the special housing unit.

Observation:

Recommendation:

19.03.09 All items entering the special housing units are searched; including food carts, clothing for exchange, property, linen, books/magazines.

Observation:

Recommendation:

19.03.10 Cell doors controlled from a remote location and remain locked at all times except when the inmate is exiting or entering the cell.

Observation:

Recommendation:

19.03.11 All cells and cell equipment are visually inspected daily.

Observation:

Recommendation:

19.03.12 High standards of sanitation are maintained in segregated housing as are required in other areas of the institution.

Observation:

Recommendation:

19.03.13 Inmates from the general population may provide sanitation and other services in the special housing unit. If allowed to do so, each worker is specifically authorized by the security chief, strip searched upon entrance and exit, and remains under direct supervision of a staff member at all times.

Observation:

Recommendation:

19.03.14 All segregated housing areas have a “911 knife”, suicide gown, suicide blanket and other equipment and supplies necessary in an emergency and in housing of inmates identified as potentially suicidal.

Observation:

Recommendation:

19.04 Inmate Services

19.04.01 Each inmate receives at least three shower opportunities per week.

Observation:

Recommendation:

19.04.02 Each inmate is allowed to exercise out-of-cell at least three times per week, for a minimum of one hour.

Observation:

Recommendation:

19.04.03 Each incident of controlled feeding status is specifically authorized by the warden/superintendent or designee with written documentation of the reason and a specified period of time, not exceeding 24 hours, before review.

Observation:

Recommendation:

19.04.04 Haircuts are available to long term, segregated housing inmates and staff document the occurrence or rejection.

Observation:

Recommendation:

19.05 Facility Design

19.05.01 The Segregated Housing Unit has a secure sally port entrance that is interlocked or for which each door is separately keyed.

Observation:

Recommendation:

19.05.02 When sufficient natural light is not available, interior lights are left on during daylight hours. Inmates are prohibited from obstructing windows or light fixtures.

Observation:

Recommendation:

19.05.03 The exercise areas for segregation inmates are searched and inspected prior to use. Special attention is paid to the condition of fence ties, metal braces and fence fabric integrity.

Observation:

Recommendation:

20. TOOL AND SENSITIVE ITEM CONTROL

Objective: To provide control and accountability for all tools and implements as well as other sensitive items stored within or that are brought into the institution for daily use.

Points of Review:

20.01 Responsibility

20.01.01 There is written policy that establishes procedures for the control of tools and sensitive items in each area of the institution. Class A (hazardous) tools are clearly defined, control procedures are specifically stated, and perpetual inventories required.

Observation:

Recommendation:

20.01.02 Qualified security staff have been designated as tool control officer and assistant tool control officer.

Observation:

Recommendation:

20.01.03 The department head of each major department is designated as the area tool control officer.

Observation:

Recommendation:

20.01.04 All staff who routinely use tools have verified, by signature, that they have read the department/institution tool control policy and procedure and understand it.

Observation:

Recommendation:

20.01.05 All contractors working inside the institution receive written instructions outlining their responsibilities regarding tool and contraband control.

Observation:

Recommendation:

20.01.06 Designated security staff conduct tool and sensitive items area inspections at least monthly.

Observation:

Recommendation:

20.01.07 Designated security staff conduct full tool control audits of all areas not less than every six (6) months.

Observation:

Recommendation:

20.01.08 Written reports documenting inspections and audits of tool and sensitive item control are submitted to the chief of security and the warden/superintendent.

Observation:

Recommendation:

20.01.09 Class A tools are used only under the direct supervision of staff.

Observation:

Recommendation:

20.01.10 When a Class A tool is missing, the staff member using/supervising the Class A tool reports this immediately to security and files a written report to the chief correctional officer.

Observation:

Recommendation:

20.01.11 When a Class A tool is missing, all inmates who had access to the tool are held at the work site until a thorough search is conducted.

Observation:

Recommendation:

20.01.12 All tools in authorized storage locations are accounted for and the inspection/ inventory is documented at the beginning and end of each workday.

Observation:

Recommendation:

20.02 *Classifying, Marking, and Storage of Tools*

20.02.01 Tools are properly classified as Class A (hazardous) or Class B (non-hazardous). Class A tools include files, knives, saw blades, ladders, ropes, extension cords, lift devices, grinders, meat hooks, and others presenting inherent safety or security risks.

Observation:

Recommendation:

20.02.02 Class A tools are stored separately from Class B tools under double lock and key.

Observation:

Recommendation:

20.02.03 All Class A tools are kept in a locked room or secure area when not in use.

Observation:

Recommendation:

20.02.04 Hacksaw blades, hilti guns, torch heads/tips, etc. are stored in the control center where a perpetual inventory is maintained.

Observation:

Recommendation:

20.02.05 All emery wheels, portable grinders, and extension cords (12 feet in length or more) are stored in a secured location when not in use and are maintained on the tool inventory.

Observation:

Recommendation:

20.02.06 All Class A tools that cannot be marked are specifically logged and inventoried daily.

Observation:

Recommendation:

20.02.07 All tools that can be marked without damage are etched with an I.D. code identifying the department, individual shop, and an individual tool number.

Observation:

Recommendation:

25.02.08 All non-Class A tools that cannot be marked without damage are kept in locked storage (not openly displayed as on a shadow board).

Observation:

Recommendation:

20.02.09 All tools that can be marked are double color-coded by department and shop.

Observation:

Recommendation:

20.02.10 Shadow boards in secured areas of the institution are used for the storage and control of most tools.

Observation:

Recommendation:

20.02.11 Where tools are shadowed, only one tool is assigned to each shadow and the number on the tool corresponds to the number on the shadow.

Observation:

Recommendation:

20.02.12 All empty shadows of tools reported missing, have tags labeled "empty" hung on the shadow or the shadow is to be removed.

Observation:

Recommendation:

20.02.13 All tools and sensitive items that are not adaptable to shadow boards are kept in locked drawers, cabinets, or other secure areas.

Observation:

Recommendation:

Tool and Sensitive Items Inventory

20.03.01 A perpetual inventory of all tools, and sub-inventory in areas where there are numerous tools, is maintained by each shop.

Observation:

Recommendation:

20.03.02 All tool inventories are signed by the tool control officer, individual department tool control officer, and chief of security.

Observation:

Recommendation:

20.03.03 Current tool inventories are typed and readily available for inspection and included in tool pouches, toolboxes, and tool kits in vehicles.

Observation:

Recommendation:

20.03.04 The tool control officer ensures that an updated inventory of all tools, including secretaries' and teachers' tools, occurs on a monthly basis.

Observation:

Recommendation:

20.03.05 Excess tools are inventoried and kept outside the institution in a secure location.

Observation:

Recommendation:

20.03.06 Tools used in any hobby craft program are inventoried, stored, and handled in accordance with regular institutional tool control policies.

Observation:

Recommendation:

20.03.07 All emergency toolboxes maintained in the control room are inventoried by designated staff on each shift.

Observation:

Recommendation:

Issuing of Tools

20.04.01 Acetylene cutting tips are checked out/in from the control room on an as-needed basis and verified present at the end of each day.

Observation:

Recommendation:

20.04.02 Hacksaw blades are mounted on rings and issued using a durable receipt system, and only in amounts necessary for one day's use.

Observation:

Recommendation:

20.04.03 Broken or worn hacksaw blades are turned in, and all parts are accounted for before a new blade is issued.

Observation:

Recommendation:

20.04.04 All ladders over four feet in length are secured in a location not accessible to inmates and are under direct employee supervision when in use.

Observation:

Recommendation:

20.04.05 Class A tools are issued to inmates only upon authorization of staff and are used by inmates under direct staff supervision.

Observation:

Recommendation:

20.04.06 When Class A tools are used by inmates, they are returned to the secure tool area by the authorizing staff.

Observation:

Recommendation:

20.04.07 When new tools are drawn for replacement, the old tool is turned in and safely disposed of in accordance with written policy.

Observation:

Recommendation:

20.04.08 A tool checkout log is maintained for all tools issued, including those used in the shop areas.

Observation:

Recommendation:

20.04.09 The tool checkout log includes:

- the date and time issued, the name of the receiving inmate or employee, tool number, and description or tool pouch number;
- the date and time returned, the issuing employee's or inmate's name, and the name of the employee or inmate receiving the returned tool.

Observation:

Recommendation:

20.05 *Food Service Implements and Sensitive Items*

20.05.01 Knives, cooking implements and tools are issued to authorized inmates only. The inmate's name and the date and time of issue and return are maintained on the checkout log.

Observation:

Recommendation:

20.05.02 When not in use knives, cooking implements and tools are securely stored in double locked cabinets and shadow boarded for frequent easy spot inventories.

Observation:

Recommendation:

20.05.03 Knives used in the food service area should be securely cabled at the work area.

Observation:

Recommendation:

20.05.04 All lost or misplaced knives shall be immediately reported to the food service manager and the shift commander. All inmates who have access to the lost items are held in the area until a thorough search is made.

Observation:

Recommendation:

20.05.05 Area shakedown and searches of "hot areas" such as the bakery, butcher's shop and vegetable preparation areas are conducted daily.

Observation:

Recommendation:

20.05.06 Foodstuffs requiring strict control are secured and a perpetual inventory is maintained. These items include yeast, nutmeg, cayenne pepper, fresh fruit, and poppy seed.

Observation:

Recommendation:

20.05.07 Non-disposable eating utensils are accounted for after each meal.

Observation:

Recommendation:

20.06 *Medical Sensitive Items – Sharps and Pharmaceuticals*

20.06.01 Procedural safeguards are in place that prevent delivery of pharmaceuticals, equipment and supplies through the general institution warehouse without proper controls.

Observation:

Recommendation:

20.06.02 Medical equipment is subject to general tool control regulations, guidelines, and monitoring. A sharp's log is fully and accurately completed on an on-going basis.

Observation:

Recommendation:

20.06.03 There is a perpetual inventory of all needles. The number of needles present in the health services unit is restricted to the number needed for the shift. All storage of hypodermic needles is in areas/cabinets of high security rating.

Observation:

Recommendation:

20.06.04 There is a perpetual inventory of all controlled substances. Controlled medications are dispensed by qualified staff. All controlled medications are stored in an area of high security rating and accessible only to medical staff except during auditing processes.

Observation:

Recommendation:

20.06.05 A perpetual inventory of the institution pharmacy is maintained and the pharmacy is audited on a regular basis by designated medical and security staff.

Observation:

Recommendation:

21. EMERGENCY PLANS

Objective: To insure that approved contingency plans are available to command staff and that these plans provide for a response to emergencies that will increase the likelihood of a successful resolution providing for the safety of all involved and the security of the institution.

Points of Review:

21.01 Responsibility

21.01.01 There is a departmental/agency policy requiring detailed emergency plans for all institutions and establishing a format and general requirements for inclusion in the institutional plans.

Observation:

Recommendation:

21.01.02 The required institutional emergency plans are reviewed and approved at least annually by the appropriate administrative/management hierarchy of the agency up to and including the agency director.

Observation:

Recommendation:

21.01.02 The institutional plans include at a minimum detailed plans for responding to the following incident types:

- External assault or terrorist activities
- Bomb threats
- Employee strikes
- Inmate escapes
- Evacuations
- Fires
- Chemical spills/hazardous material incidents
- Hostage situations
- Medical emergencies or epidemics
- Natural disasters
- Riots and disorder

Observation:

Recommendation:

21.02 ***Plan Requirements***

21.02.01 Institutional plans clearly establish the command structure in emergencies as well as specifically how command is assumed and/or transferred and for the security of command.

Observation:

Recommendation:

21.02.02 Institutional plans include specific requirements and protocols for managing the operational, planning, administrative and logistical functions during an emergency, particularly one of extended duration.

Observation:

Recommendation:

21.02.03 In situations where staff safety may be threatened, pre-designated “safe-havens” are specified in the plan and provisions made to insure that all staff are aware of the specific locations for both their safety and to facilitate accounting for all staff.

Observation:

Recommendation:

21.02.03 Institutional plans contain emergency post orders and responsibility check lists for staff assigned to each essential primary emergency response function.

Observation:

Recommendation:

21.02.04 Institutional plans include specific, current notification call lists, an automated substitute, and/or other reliable contact method, e.g. pagers, for institutional management, agency executive staff, institutional emergency response staff, and appropriate local and state law enforcement agencies.

Observation:

Recommendation:

21.02.05 Written agreements are required and available for any emergency response plan component service that is provided by an entity external to the facility, e.g. local fire

department, hospital, etc., Such agreements are comprehensive and specify the service to be provided, any limitations, etc.

Observation:

Recommendation:

21.02.06 Institutional emergency plans are securely stored and have restricted access. They are, none-the-less, accessible during an emergency to designated staff responsible for their implementation.

Observation:

Recommendation:

21.02.07 During an emergency as appropriate and indicated, all external communication systems, e.g., inmate phone system, can be controlled and/or disabled from a secure location.

Observation:

Recommendation:

21.02.08 There is a reliable method of positively accounting for the absence or presence of all staff and other non-inmates within the institutional perimeter at any time.

Observation:

Recommendation:

21.02.09 There is command center pre-designated in a highly secure location preferably external to the secure perimeter that is equipped with sufficient communication capability to manage an emergency situation to include telephones, computers, and radios with talk around and mutual aid capability. Additionally the center should contain detailed current maps of the facility and surrounding area as well as blue prints of all aspects of the physical plant.

Observation:

Recommendation:

21.02.10 The institution has an emergency response team capability of sufficient number for the institution's population, custody, mission, etc. Team members are readily available, competent with both lethal and less lethal weapons and munitions, and train at least

monthly in accordance with carefully designed lesson plans. External annual assessments of proficiency are required.

Observation:

Recommendation:

21.03 *Training*

21.03.01 All staff receive mandatory annual training on individual staff requirements and expectations during an emergency. This training is tailored to staff in various departments and areas.

Observation:

Recommendation:

21.03.02 Emergency drills and simulations are conducted on a regular basis but no less than quarterly. These drills/simulations are in addition to the normally required fire evacuation drills. Examples of such drills include tabletop exercises for management and supervisors, actual escape simulations involving apprehension teams and local law enforcement and/or alert calls for response teams to test availability and response times.

Observation:

Recommendation:

21.03.03 An annual emergency training drill/simulation is required of a scope and magnitude sufficient to involve other surrounding institutions and central office/agency staff. All levels of command and support are tested.

Observation:

Recommendation: