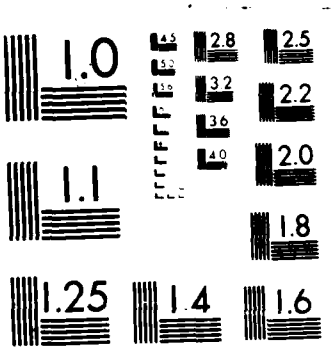
AD-A179 899 IMPROVING INSTALLATION LEVEL CLASSIFIED INFORMATION PROTECTION PROGRAMS(U) AIR COMMAND AND STAFF COLL MAXWELL AFB AL A T AKEO APR 87 ACSC-87-0040 1/1

UNCLASSIFIED F/G 15/4 NL



AIR COMMAND AND STAFF COLLEGE

STUDENT REPORT

IMPROVING INSTALLATION LEVEL CLASSIFIED INFORMATION PROTECTION PROGRAMS

MAJOR ALVIN L. K. AKEO 87-0040

"insights into tomorrow"

DISCLAIMER

The views and conclusions expressed in this document are those of the author. They are not intended and should not be thought to represent official ideas, attitudes, or policies of any agency of the United States Government. The author has not had special access to official information or ideas and has employed only open-source material available to any writer on this subject.

This document is the property of the United States Government. It is available for distribution to the general public. A loan copy of the document may be obtained from the Air University Interlibrary Loan Service (AUL/LDEX, Maxwell AFB, Alabama, 36112) or the Defense Technical Information Center. Request must include the author's name and complete title of the study.

This document may be reproduced for use in other research reports or educational pursuits contingent upon the following stipulations:

-- Reproduction rights do not extend to any copyrighted material that may be contained in the research report.

-- All reproduced copies must contain the following credit line: "Reprinted by permission of the Air Command and Staff College."

-- All reproduced copies must contain the name(s) of the report's author(s).

-- If format modification is necessary to better serve the user's needs, adjustments may be made to this report--this authorization does not extend to copyrighted information or material. The following statement must accompany the modified document: "Adapted from Air Command and Staff Research Report (number) entitled (title) by (author) ."

-- This notice must be included with any reproduced or adapted portions of this document.

REPORT NUMBER 87-0040

TITLE IMPROVING INSTALLATION LEVEL CLASSIFIED INFORMATION PROTECTION PROGRAMS

AUTHOR(S) MAJOR ALVIN L. K. AKEO

FACULTY ADVISOR MAJOR PAT EVANS, ACSC/3822 STUS

SPONSOR Colonel Peter A. Colangelo, HQ TAC/SPD

Capt Marvin E. Lands, TISD/SITT

Submitted to the faculty in partial fulfillment of requirements for graduation.

AIR COMMAND AND STAFF COLLEGE
AIR UNIVERSITY
MAXWELL AFB, AL 36112

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE

A179892

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT **STATEMENT "A"** **Approved for public release;** **Distribution is unlimited.**
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) 87-0040	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION ACSC/EDCC — 6b. OFFICE SYMBOL (*If applicable*)	7a. NAME OF MONITORING ORGANIZATION
6c. ADDRESS (*City, State and ZIP Code*) Maxwell AFB AL 36112-5542	7b. ADDRESS (*City, State and ZIP Code*)
8a. NAME OF FUNDING/SPONSORING ORGANIZATION — 8b. OFFICE SYMBOL (*If applicable*)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (*City State and ZIP Code*)	10. SOURCE OF FUNDING NOS. PROGRAM ELEMENT NO. — PROJECT NO. — TASK NO. — WORK UNIT NO.
11. TITLE (*Include Security Classification*) IMPROVING INSTALLATION LEVEL	
12. PERSONAL AUTHOR(S) Akeo, Alvin L. K., Major, USAF	
13a. TYPE OF REPORT — 13b. TIME COVERED FROM ____ TO ____	14. DATE OF REPORT (*Yr., Mo., Day*) 1987 April — 15. PAGE COUNT
16. SUPPLEMENTARY NOTATION ITEM 11: CLASSIFIED INFORMATION PROTECTION PROGRAMS	
17. COSATI CODES FIELD — GROUP — SUB. GR.	18. SUBJECT TERMS (*Continue on reverse if necessary and identify by block number*)

19. ABSTRACT (*Continue on reverse if necessary and identify by block number*)

Recent DoD and USAF reviews of security policies and practices have uncovered serious deficiencies in security programs developed to protect classified and sensitive information. Organizing security program managers and command oversight at the installation level offers one alternative to improving the effectiveness of USAF security programs.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☒ DTIC USERS ☐	21. ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED
22a. NAME OF RESPONSIBLE INDIVIDUAL ACSC/EDCC Maxwell AFB AL 36112-5542	22b. TELEPHONE NUMBER (*Include Area Code*) (205) 293-2483 — 22c. OFFICE SYMBOL

DD FORM 1473, 83 APR — EDITION OF 1 JAN 73 IS OBSOLETE.

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE

PREFACE

It's tough to get people motivated over security. Whether the profession is flying on behalf of national defense or private enterprise, good security is expensive. In the military, the cost is often measured in time "wasted" at restricted area entry control points or frustration in complying with the 100-step rituals associated with handling or using classified information. In the private sector, security is measured in terms of the expenses involved in hiring security personnel and equipment to protect aircraft, air terminals, and passengers, and extensive ground time to conduct passenger and baggage checks.

Ideal security is effective and unobtrusive. Ideal security is expensive security because it requires a scarce commodity: leadership involvement. Leadership involvement that drives total unit commitment to security policies and procedures that become second nature and--in becoming natural--unobtrusive.

The Stillwell Commission launched some scathing criticism at DoD security policies and practice; a few appear as chapter lead-offs. The Commission moderated the impact of their comments at the close of each area reviewed, but I want to place my comments at the outset of this effort. By and large, the people who work at protecting classified and sensitive information are some of the most dedicated and professional that we have. I've been watching them, and working with them, for almost 24 years. I am amazed at their resilience, since it seems that most often, their accomplishments have been constrained only by our indifference.

This paper is an entreaty to break the restraining indifference by organizing both ends of the security program process: program organization and administration at the base of the effort; and command emphasis on program objectives at the forefront. I don't see any other way or security effectiveness to steadily improve and stabilize.

Finally, in prosecuting the academic portion of this study, I may have departed from the basic idea that led to the development of this study. To make sure that readers know my heart was in the right place, even if I didn't get it all right, I want to capsulize my intent very briefly. Security programs must be unified for management focus

toward a single objective. A single objective that can be achieved by following a multiple of paths, represented in the varied security programs in existence, that converge at a common objective of denying valuable information to our enemies. The technological lead that has long enabled us to moderate the numerical superiority of Soviet forces is rapidly diminishing. Much of it as a consequence of poor security practice. We can't afford to squander the edge we possess by neglecting the very programs that help to sustain that edge.

I want to thank Col Peter A. Colangelo and Capt Marvin E. Landa, who are serving HQ Tactical Air Command at Langley Air Force Base, Virginia. I didn't solve the original problem you both posed, but the one I did work might serve until DoD and the Air Staff work out the huge knots tied into classified information protection programs. I also want to thank Mr George Paseur at the Office of Security Police for his encouragement and incisive insight.

ABOUT THE AUTHOR

Major Al Akeo brings a strong security background to this research project. As a member of United States Air Force Security Service (Electronic Security Command) from 1964 to 1973, he participated in all of the security programs discussed in this study as well as special intelligence and sensitive compartmented information programs. Following his commissioning in 1974, Major Akeo served as the OIC, Weapons Systems Security, where he first entered the Personnel Reliability Program, then as the OIC, Administration and Reports, at Torrejon Air Base, Spain, between 1975 and 1978. While serving in the latter position, he managed and provided oversight for the installation's Information, Industrial, and Resources Protection Programs. During his assignment as the Chief, Security Police, Wheeler Air Force Base, Hawaii, between 1980 and 1981, he directed all security police security programs and served as the installation Information Security Program Manager. He attended the School of Criminal Justice, Michigan State University, East Lansing, Michigan, during 1982 and 1983, and was awarded the degree Master of Science, with a concentration in Security. In partial fulfillment of his degree requirements, he combined academic and field research to develop security plans and procedures for the personnel, facilities, and information systems resources of the Social Security Administration, West Michigan. Most recently, Major Akeo served as the Chief, Law Enforcement Branch, HQ Tactical Air Command (SP) and as an Inspector, HQ Tactical Air Command (IG). While serving as an inspector, Major Akeo was selected to serve as the Command's project officer for the Secretary of Defense-Directed Command Security Inspection (SDCSI) frequently referenced in the study. He is the authority on TAC's execution of, and performance in, the SDCSI.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

REPORT NUMBER: 87-0040

AUTHOR: MAJOR ALVIN L. K. AKEO, USAF

TITLE: IMPROVING INSTALLATION LEVEL CLASSIFIED INFORMATION PROTECTION PROGRAMS

I. PROBLEM. To improve the effectiveness of USAF installation level classified information protection programs.

II. BACKGROUND. Recent unauthorized disclosures of classified information to the Soviets, as well as the findings of a 1985 DoD level committee, signal the need for improvement in the programs designed to protect classified information. Selected findings in the DoD committee report further suggest that better organization of, and increased command oversight on, classified information protection programs represent a potent approach to improving security program performance. Virtually all substantive "fixes" keyed to the DoD committee's findings appear to be long term.

III. PROPOSAL. With the exception of traditionally excluded programs (e.g., SCI, DIA administered areas), installation level security program managers should be organized into a classified information protection committee (CIP). The committee should be tasked to identify key issues and problems across the range of programs active on the installation. The committee should then be matched to an established executive group, like the Base Security Council, to present the issues and enable installation executives to guide and direct efforts and resources in improving program performance.

IV. ADVANTAGES. The proposal has high potential for bringing command emphasis to bear on important, but often neglected, security issues. In addition, the proposal capitalizes on using existing resources to implement a cost free alternative.

V. RECOMMENDATION. The proposal should be offered as an option for Base Security Councils. Alternatively, the proposal could be tested at selected sites and the results evaluated to support retention or rejection of the program.

Chapter One

THE PROBLEM AND ITS SIGNIFICANCE

> Security involves active and passive defensive measures and the denial of useful information to any enemy. To deny any enemy knowledge of friendly capabilities and actions requires a concerted effort in both peace and war.
>
> Basic Aerospace Doctrine (7:2-6)

> Insufficient attention has been given to the overall purpose of security as it relates to organizational mission, to observation of subordinates' security performance and insuring that basic security principles are adhered to in practice. The key to genuine improvement in DoD's security posture is continuing, pervasive oversight by commanders and supervisors at all levels.
>
> Stillwell Commission (9:14)

Introduction

The obvious disparity between the cited dictum of United States Air Force (USAF) doctrine and the critical quote by the Commission to Review and Evaluate DoD Security Policies and Practices (Stillwell Commission) forms the basis for this paper. The citations similarly focus on preserving USAF force capabilities through the denial of information to an enemy. The doctrinal statement, moreover, appears to establish a security task or capability, while the citation from the Stillwell Commission pointedly criticizes the manner in which the task is being executed. The irony of finding security arrayed among the "major truths" of aerospace doctrine, but assessed as ineffective because of poor command oversight, is at once explicable and inexplicable. Explication begins and ends with accountability. In general, the classified information protection programs developed to support aerospace security lack objective focus and suffer from fragmentation of responsibility. At the Department of Defense (DoD) level, security policy responsibilities for the programs addressed

in this paper are shared among an assistant secretary of defense, a deputy assistant secretary of defense, and an under secreatary of defense (9:82). At the Air Staff level, DoD policies are transformed into programs by elements of an assistant chief of staff, a deputy chief of staff, and the USAF Inspector General. Air Staff counterparts at the major command (MAJCOM) level, and down through the organizational chain to installation level managers, complete the program administration bureaucracy. There is no point along the functional chain extending from the DoD staff to the installation manager where a central, organizing agency has established a central objective for the individual programs (9:83). As a consequence, individual security programs are often pursued as ends in themselves, without clear regard for the manner in which they impact, and are impacted by, other programs (5:3). The issue of greatest impact, however, is the isolation of installation leaders from overall direction of installation security programs. None of the security programs in this study directly address installation command responsibilities <u>across</u> the range of security programs administered on USAF installations. Hence, while virtually all security programs establish detailed requirements for program administration and measurement of effectiveness (either through local or higher headquarters inspections), responsible commanders are not generally included in the process of ensuring "across the board" effectiveness among all security programs. As a consequence, doctrinal entreaties for "concerted effort" on security issues, and DoD level demands for improved command oversight for security activities, have been thwarted. Failures in security programs have been spectacularly highlighted in headlines revealing former Navy veteran John Walker's compromise of classified information to the Soviets and similar acts by the National Security Agency's Ronald Pelton. Appreciation of this systemic security program fragmentation illuminates the ironical difference between the tasks implied in doctrine and the inadequacies noted in the programs developed to fulfill the tasking. What remains inexplicable, however, is the glaring contrast between the doctrinal exigency and practical inadequacy noted in the lead citations.

There have been a variety of responses to the apparent shortcomings in our security efforts. In 1985, the Secretary of Defense chartered the Stillwell Commission to "identify any systemic vulnerabilities or weaknesses in DoD security programs, including an analysis of lessons learned from incidents which have occurred recently, and make recommendations for change as appropriate" (9:113). In its report, the commission identified 63 wide-ranging recommendations for improving extant security programs. Following a USAF-wide Secretrary of Defense Directed Command Security Inspection (SDCSI) generated by a Stillwell Commission recommendation, the USAF proposed correcting

security program deficiencies through immediate updates in guidance (3:--). HQ Tactical Air Command (TAC), in its SDCSI report, suggested radically reorganizing all security personnel and regulations under a more effective structure (5:3). However, although the Stillwell Commission and HQ TAC reports recommended improvements in areas related to this study, neither report centered on satisfying the previously discussed doctrinal desire for concerted effort and the commission's concern over insufficient command oversight. As a result, a broad area relating to doctrinal and practical security issues remains open to effective, innovative effort.

The Problem

The purpose of this paper is to develop a method for improving the effectiveness of USAF security programs, ensuring "concerted effort" and command oversight are fundamental to the proposed solution. The hypothesis of this study is that a new concept for managing security programs and innovative use of an approrpiate executive committee, such as the Base Security Council (BSC) (4:--), can result in an acceptable solution. The combination of the new concept and the use of the BSC is referred to as the Classified Information Protection (CIP) Program. A corresponding objective of this study is to encourage implementation of the CIP Program.

Delimitations of the Study

First, the problem addressed in this study is probably applicable to the management of security programs throughout the USAF. However, the overall intent is to impact installation level security programs. In addition, since the primary documentary examples are essentially TAC-based, the problem and recommended solution may only be relevant to TAC.

Second, DoD, Air Staff and MAJCOM level actions that may impact on the security program aspects addressed in this paper appear to be either long-term or non-existant. Thus, this study was undertaken to provide installation leadership an interim, cost effective management option that can be immediately implemented.

Finally, this study focuses on peacetime security and is intended to affect only the following programs:

Communications Security (AFR 100-46)

Hostile Human Intelligence Threat (AFR 205-57)

Industrial Security (AFR 205-4)

Information Security (AFR 205-1)

Information Systems Security (AFR 700-10)

Operations Security (AFR 55-30)

Tempest (AFR 56-50)

Importance of the Problem

Developing and sustaining effective security programs is essential to maintaining the security capability mandated in aerospace doctrine. A solution that contributes to USAF security contributes to the overall security of the United States and its interests.

Although the topic of this study does not address the full range of security issues encompassed in aerospace doctrine, effective execution of these limited aspects of security would certainly contribute to the overall security capability envisioned in doctrine.

Methodology/Data

First, this study proceeds on the basis of the following assumptions and groundwork:

-- Aerospace doctrine establishes implicit security tasks (7:2-6).

-- The security programs criticized by the Stillwell Commission (9:--) were developed, at least in part, to satisfy the security tasks implied in aerospace doctrine.

-- Research in this area is virtually non-existant (9:13,86-88; 10:32). Consequently, corrective conceptual and procedural recommendations are often asserted without academic precedent.

Second, in executing this study, USAF directives, HQ TAC and USAF SDCSI reports, and the results of informal interviews are cited in support and explication of the problem hypothesis (see "The Problem", above). Fundamentally, however, this study heavily relies on experience, common sense, and the use of available resources to make an important program work better.

Third, intellectual comprehension and acceptance of the CIP concept and commitment of an executive group, like the

BSC, in resolving the problem addressed is essential to this effort.

Finally, though this paper separates the CIP concept and the BSC discussion into separate chapters, the overall intent of this study is to portray the CIP concept and the use of the BSC as a unity.

Organization of the Project

This paper is presented in three major sections. In Chapter Two, a case is made for adopting and applying a security program organizing concept (CIP) to the seven programs previously enumerated. Using BSCs as an integral part of the CIP Program to bring "concerted effort" and command oversight to USAF security programs is addressed in Chapter Three. Finally, Chapter Four identifies basic implementation considerations for the CIP Program and closes with a summary of the proposed solution.

Chapter Two

AN ORGANIZING CONCEPT FOR USAF SECURITY PROGRAMS

> Few [organizations and offices] have consolidated all aspects of security policy under one official. Moreover, security officers are often "buried" far down in the organization and consequently have neither the opportunity to bring major problems or recommendations to top management attention nor the authority to conduct effective oversight and deal with deficiencies.
>
> Stillwell Commission (9:81-82)

Introduction

USAF security programs are not organized for "concerted effort" and command oversight. Neither the Stillwell Commission nor the USAF SDCSI report addressed effective reorganization below the DoD level as a means of improving security programs. The HQ TAC report, however, recommended radical reorganization of security program regulations and personnel to achieve more effective centralized management (5:3). In part, the HQ TAC suggestion stemmed from an acute reaction to the pervasive fragmentation of security responsibilities (9:81-85) previously noted. HQ TAC interpreted the resulting proliferation of regulations and supplements as contributors to confusion, redundancy, and a loss of focus on the overall objective of the DoD and USAF programs (5:3).

This chapter discusses a method for improving installation level management of USAF security programs. Hypothetical program manager and senior leadership points of view are presented and the CIP Program concept is outlined.

Installation Level Management

Each of the security programs identified in Chapter One is administered by a separate installation program manager. Program managers, and monitors in each of the units on the installation, work doggedly to turn organizational

indifference toward security requirements into minimal compliance with program requirements. Depending on the specific program, managers range in rank from technical sergeant to ranks not normally above major. Managers at all levels, but particularly at the bottom end of the rank scale, normally experience significantly greater difficulty in executing their programs. In addition, the typical manager is almost always behind on the huge and varied workloads normally associated with administering the installation program. The manager works in virtual isolation, without sustained, organized support, to make his program work and feels fortunate if the overall program satisfies mere program compliance requirements. In summary, the typical manager knows what to do and attempts to execute program requirements. However, the sheer mismatch in available time and manpower resources versus work requirements, in combination with "customer" resistance and reluctance, makes the program manager's task an arduous, uphill battle.

Installation Leadership

By and large, installation senior leaders are not in an effective security program oversight loop. For example, although most compromises of classified information normally result in some leadership involvement, and some commanders review security program reports on their individual units from time to time, senior leaders do not regularly see a cross section of the installation's performance across the range of active security programs. Senior leaders, then, normally never confront broad-based and broadly applicable security program issues.

An Organizing Security Concept

An overall, organizing element is required to bring cohesiveness to the segmented entities of individual security programs, managers, and leadership. In the context of this project, the organizing element should serve at least two purposes. It should bring individual security programs and their managers onto common ground, where common program needs and problems can be discussed, and it should enable senior leadership to deal with major security program problems. The CIP concept can serve both purposes.

The CIP concept is a straightforward effort to design "concerted effort" and command oversight into security program execution. Under the CIP concept, an umbrella management progam encompasseses individual programs, like COMSEC and OPSEC, as component parts. The resulting CIP Program enables senior leadership to look at, and measure the relative health of, all component programs, at a single

sitting, through a review of previously identified program issues.

Under the CIP Program, security program managers meet as a committee to identify significant indicators and measurements of program vitality. The committee then analyzes and organizes the information for presentation to installation leaders. Leaders, for their part, would direct necessary supporting effort, and otherwise apply command emphasis and oversight, to assure program vitality. For instance, virtually all security programs require newcomer briefings for all personnel within a specified number of days of arrival at a new installation. As part and parcel of the newcomer briefing requirement, there normally exists a companion requirement for a supplementary, annual briefing. Since these two requirements constitute clear and measurable regulatory requirements, they tend to constitute the criteria that inspectors use to evaluate the program. Consequently, the collective of individual program managers--functioning as a CIP Program Committee--could decide to identify newcomer briefing statistics as one common measure of installation security program vitality. In this example, the managers may also decide to broaden the briefing to discuss whether MAJCOM inspectors ought to look at briefing statistics as a reliable measurement of program success. In illustration, the CIP Program Committee may be able to demonstrate that the briefings are ineffective because new arrivals are normally preoccupied by at least 50 topics of inestimably greater importance and interest than the typical newcomer's briefing. Further, the CIP Program Committee may be able to substantiate switching to semi-annual testing as a better way to achieve and measure program effectiveness. Finally, using the same example, the committee could develop their findings into a leader-sponsored change to applicable directives. In essence, the CIP concept, manifest in the CIP Program committee, would provide senior leaders an opportunity to directly impact security issues and direct concerted effort toward resolving problems.

The CIP Program means establishing, then maximizing, the overall objective of the collective of component security programs: denial of useful information to any enemy. Next, the CIP Program involves looking at the component programs to see how well the objective is being achieved. Finally, the CIP Program means taking a broad, management look at significant security program issues, and getting "concerted effort", through command direction and oversight. The non-directive, informational USAF OPSEC Guide (8:3), contains several excellent suggestions on Operations Security Boards that could be applied to the CIP Program Committee.

To function most effectively, however, the CIP Program concept should be merged with an appropriate senior leadership forum and the BSC appears custom made for the job.

Chapter Three

THE CIP PROGRAM IN THE BASE SECURITY COUNCIL (BSC)

> [S]ome commanders and supervisors show a clear disdain for security, leaving compliance to clerks and secretaries. When security requirements become an impediment, they are ignored either for reasons of personal convenience, to facilitate job performance, or, perhaps, for political reasons. Whatever the reason, such attitudes have a debilitating impact on subordinates and on the success of the program as a whole.
>
> Stillwell Commission (9:80)

Introduction

This chapter discusses including the CIP Program under the BSC, a powerful, decision-making body established to provide command oversight to the protection of USAF warmaking resources (4:1-1). It discusses how and why the BSC works effectively and suggests how the CIP Program can be grafted onto the BSC framework to provide concerted effort to aerospace security programs. Although the BSC is specifically addressed in this study, other similarly perceived and conceived executive groups would work.

The Stillwell Commission did not address "concerted effort", in the context of this study, as a means of improving the overall effectiveness of security programs. The HQ TAC report suggested creating a "super" installation security manager who would be responsible for all security programs, coordination with local security managers, and required coordination with program managers above the installation level (5:3). In addition, HQ TAC recommended strengthening the position of individual unit security managers to ensure the availability of time to work security program requirements (5:9). The HQ TAC focus on centralizing responsibility represents a potent suggestion. However, this same suggestion could inadvertantly neutralize essential command oversight over security progams. Extant demands for "concerted effort" and command oversight with

respect to security program issues begs development of a more encompassing alternative.

"Concerted Effort" in the USAF

"Concerted effort" certainly suggests broad, but effective, participation in security activities. Within the USAF, concerted effort can easily be equated to working group and committee approaches to problem solving. Group effort is a way of life in the USAF. Some work has been done on the uses of committees (2:199-229; 11:--), but in the context of the USAF, academic prescriptions and proscriptions are moot: the USAF indorses committees as an accepted way of getting work done by broad-based use of committees. Promotions, policies, finances, charitable contributions, war planning and a myriad other issues are directly worked, or fundamentally supported, by committees. At the installation level, a committee system has been developed to work certain kinds of security issues.

Base Security Councils

The BSC is effective because of its purpose and the authority of its membership. The Air Force Physical Security Program mandates a BSC on each installation that supports priority resources (4:1-1). In general, priority resources are those resources directly bearing on the USAF's fighting capability, such as alert aircraft and supporting command and control systems.

The BSC is a decision making body and its membership is selected by the senior tactical commander on the installation. A typical BSC is chaired by the vice wing commander while wing deputates and selected wing staff personnel complete the membership. The Chief, Security Police normally plans, conducts, and records the business of the council. (4:1-1) If problems or requirements relating to priority resources arise, the issue goes to the BSC and the BSC fixes it. Period.

The BSC is decisive and effective for several good reasons. First, the overriding concern of the council is support of wartime capability. Find wing leadership lagging on wartime capability and you've likely found a command vacancy waiting to happen. For the wing commander, maintaining flying "readiness" comes first. Making sure the platforms are there to fly, particularly in the current pervasive, non-specific terrorist threat environment, is an issue tucked tightly in the slipstream of flying mission readiness. Second, the BSC is <u>power</u>. The people who own everything and everybody on the installation are in the BSC. If the council wants or needs to do something, it gets done.

Third, numerous action items are worked and briefed at the BSC and given the make-up of the council, failure to progress on agreed upon fixes is not frequently tolerated.

The CIP Program in the Base Security Council

Adopting the CIP Program concept and committing the BSC to the CIP Program oversight requires an act of faith. The CIP Program is a relatively unprecedented (even given a similar, though narrower OPSEC approach (8:3)) idea that makes good sense.

The BSC is ready-made for the CIP Program: the right people, power, results-orientation. In addition, the kind of thinking that goes on in the BSC fits, too. The council thinks, talks, and does security. A different kind of security than the CIP Program addresses, but security, nevertheless. On one hand, the BSC primarily works at protecting physical assets, such as aircraft and command posts. Alternatively,the CIP Program not only works at securing physical assets, but also concentrates on securing floppy disks, paper, procedures, radio transmissions, pieces of equipment that "radiate," and, just as importantly, the "stuff" inside people's heads. Above all, commitment of an executive group to security program oversight would signify decisive leadership support for security, averting the "debilitating impact" (9:80) leadership neglect has fomented.

Regardless of the differences, however, the council is oriented toward security and getting results. But, what ought the BSC do for the CIP Program? Council meetings are expensive meetings; council time represents premium leadership time. The council normally meets twice a year, much of the agenda is prescribed, and committees work out the issues to minimize impinging on expensive executive time. To preserve the efficacy of the council, how ought the CIP Program integrate with the BSC?

Chapter Four

IMPLEMENTATION AND SUMMARY

> As bureaucratic and mundane as security requirements sometimes appear, they offer the only systematic means available to protect and preserve the defense community's triumphs and advances, over time. Security must be given its fair share of serious attention and its fair share of resources.
>
> Stillwell Commission (9:16)

Introduction

This chapter addresses some basic recommendations on implementing the CIP Program/BSC package. Hereafter, the term CIP Program is used to refer to this package. In addition, the chapter comments on Air Staff feedback on the study and closes with a brief summary of the project.

Integrated Implementation

The CIP concept and the commitment of the BSC must be implemented as an integral package to achieve optimal results. Developing the CIP concept (organizing security program managers into a committee, identifying issues for presentation to senior leaders, etc.) in isolation from the kind of senior leadership support inherent in the BSC would be counterproductive. Without strong leadership support, the CIP Program Committee would be no more than collective whistling in the dark. Program managers know what isn't working and probably know how to fix it. Collectively, the program managers require command sponsorship of changes designed to improve program effectiveness and decisive support to break through organizational resistance and indifference to program objectives and requirements.

On the other hand, placing security program issues in the BSC without the structure that the CIP concept imparts would also result in less than optimal results. The organizing effect of CIP Program Committee pre-planning, identification of issues, and pre-council preparation

ensures timely and concise presentation of issues, rapid progress to decision points, and efficient use of executive time.

Implementation of the CIP Program and commitment of the BSC must be seen as an integral package. Use of the term CIP Program should mean "the security program management committee of the BSC."

Installation Level Implementation

At the installation level, the crucial decision is whether to adopt the CIP Program. The program will probably not be sold on academic merit. The Stillwell Commission found that academic endeavors do not normally extend to the topics discussed in this study (9:13,86-88). As a consequence, there is very little direct research to support the study. In a related vein, however, social scientists suggest that we sometimes make choices on the basis of experience and preference rather than authoritativeness (research) (1:42). In this instance, installation leadership and management must bring common sense and experience, versus academic authoritativeness, to bear in deciding whether to use the CIP Program.

The following should be considered in implementing the CIP Program.

1. Determine whether the CIP Program can improve the effectiveness of installation security programs. One useful method is to review progress in correcting the deficiencies identified during the installation's SDCSI. If solid progress has been made and the corrective actions reflect "concerted effort" and command oversight as integral aspects of effective security, then the installation should "round file" this study. However, indecision or doubt over solid progress should be a motivator to try the CIP Program.

2. After commitment to the CIP Program, senior leadership should direct installation security program managers to conduct an organization meeting of the CIP Program Committee of the BSC. Guidelines for the organization meeting, and all subsequent meetings, should include identification of significant security program issues for presentation to the BSC. The issues nominated for BSC presentation should address problems in the "pass/fail" and effective/ineffective aspects of security program administration and represent opportunities for senior leadership to apply command oversight to the direction and progress of corrective actions. Issues should be presented in a manner to allow an executive decision, if required, at the close of the presentation.

3. The CIP Program committee should be chaired by the installation Chief, Security Police or the Director, Information Systems, or co-chaired by both. Between them, they manage five of the seven programs nominated for inclusion in the program. Because of the overall BSC responsibilities the Chief, Security Police already shoulders, the Director, Information Systems, should probably chair the committee.

4. Ensure the CIP Program Committee works toward mutual support among the security programs administered on the installation and that the BSC continually exerts emphasis and influence through full participation in security program problem resolution.

5. Notify MAJCOM security program managers that the installation has adopted the CIP Program.

In addition to the above, installation leaders should bear in mind that the proposed solution is virtually cost free and flexible. Subject area specialists for the CIP Committee already exist in the security program managers already assigned to the installation, and a senior leadership forum already exists in the BSC.

MAJCOM Implementation

The MAJCOM offices of primary responsibility (OPR) for the security programs identified in Chapter One should review this study and consider implementation throughout the command; however, action at the MAJCOM level is not neccessary. The CIP Program should not be mandated unless MAJCOM and installation leadership support establishing a mandatory program. MAJCOM wing commanders' conferences or similar events are excellent test beds for presenting the topic.

Short of an attempt to present the topic for MAJCOM and installation leadership acceptance, the MAJCOM program managers could still "permissively" support the program. The CIP Program could be authorized as a BSC option in the MAJCOM supplement to AFR 207-1, Air Force Physical Security Program. Alternatively, the program could be implemented on a test basis at selected sites and the results used to determine whether to retain the program for broader, mandatory use, or to reject the program.

The impact of each alternative appears self-evident. Early, mandated implementation of the program would create an IG inspection vulnerability for a new program requiring a "shakedown." Optional or test implementation, however, would allow installation leadership and management an opportunity to experiment with a potentially beneficial

program, and, in the process, could result in the development of a research base to measure program merit.

HQ USAF and HQ TAC Comments

Representatives from the HQ USAF and HQ TAC OPRs for most of the security programs identified in this study see potential in the CIP Program (12:--; 13:--; 14:--; 15:--). Their sentiments were probably best captured by George Paseur (who testified before the Stillwell Commission) in these informal remarks regarding this project: "Your efforts to organize and improve the effectiveness of our security programs is a good one. We need more ideas and more effort in this area" (15:--). For both staffs, the CIP Program approach certainly represents a less radical approach than some of the massive changes previously discussed (5:--; 9:--).

Summary

> Once you create an idea, it takes on a life of its own.
>
> James M. Buchanan
> 1986 Nobel Laureate for Economics

Thoughtful implementation of the CIP Program along the guidelines suggested in this study will satisfy aerospace doctrine and DoD mandates for "concerted effort" and command oversight in security activities. Implementation of the CIP Program would contribute to the central purpose of this study: overall improvement in the effectiveness of USAF security programs.

Above all else, however, this study was intended as a heuristic approach to problem solving. If it stimulates thought and action processes that give rise to a better, broader solution, then an even better purpose has been served.

BIBLIOGRAPHY

A. REFERENCES CITED

Book

1. Cohen, David K. and Charles E. Lindblom. Usable Knowledge: Social Science and Social Problem Solving. Binghamton, New York: Yale University Press, 1979.

2. LeBreton, Preston P., and Dale A. Henning. Planning Theory. Englewood Cliffs, NJ: PRENTICE-HALL, INC., 1961.

Official Documents

3. US Department of the Air Force. Air Force Inspection and Safety Center. "Report on Secretary of Defense-Directed Command Security Inspection PN 86-614 3 FEB - 9 SEP 86," report. Norton Air Force Base, California, 14 October 1986. FOR OFFICIAL USE ONLY. This is a PRIVILEGED DOCUMENT not releasable in whole or in part to parties or agencies outside the Air Force without the express approval of the Secretary of the Air Force.

4. US Department of the Air Force. (C) The Air Force Physical Security Program (U). AFR 207-1. Washington, DC: Government Printing Office, 1981. "Unclassified information only used from this source."

5. US Department of the Air Force: HQ Tactical Air Command (CS). "Final Report, Tactical Air Command and TAC Gained ANG Units SECDEF-Directed Command Security Inspection (SDCSI), PN 86-614," letter. Langley Air Force Base, Virginia, 3 July 1986. FOR OFFICIAL USE ONLY. This is a PRIVILEGED DOCUMENT not releasable in whole or in part to parties or agencies outside the Air Force without the express approval of the Secretary of the Air Force.

6. US Department of the Air Force. The Resources Protection Program. AFR 125-37. Washington, DC: Government Printing Office, 6 May 1982.

7. US Department of the Air Force. United States Air Force Basic Doctrine. AFM 1-1. Washington, DC: Government Printing Office, 1984.

8. US Department of the Air Force. USAF OPSEC Guide. AFP 55-36. Washington, DC: Government Printing Office, 9 July 1985.

9. US Government. Office of the Secretary of Defense. Keeping the Nation's Secrets: A Report to the Secretary of Defense by the Commission to Review DoD Security Policies and Practices. Washington, DC: Government Printing Office, 1985.

Unpublished Materials

10. Akeo, Alvin L. K. "Social Security Administration Field Office Security Plans." Policy Paper, School of Criminal Justice, Michigan State University, 1983.

11. Gluck, Fred. "Committees in Organization". Master's Thesis, University of Texas, 1958.

Other Sources

12. Air Staff Officer, Maj, USAF. Technology and Security Division, Assistant Chief of Staff for Information Systems, HQ United States Air Force, Washington, DC. Telecon, 6 February 1987.

13. Colangelo, Peter A., Col, USAF. Deputy Chief, Security Police, HQ Tactical Air Command, Langley Air Force Base, Virginia. Telecon, 6 February 1987.

14. Landa, Marvin E., Capt, USAF. Director, Security, Deputy Chief of Staff, Communications Computer Systems, HQ Tactical Air Command, Langley Air Force Base, Virginia. Telecon, 6 February 1987.

15. Paseur, George. GM-15, USAF. Director, Information Security, Office of Security Police, HQ United States Air Force, Kirtland Air Force Base, New Mexico. Telecon, 6 February 1987.

B. RELATED SOURCES

Official Documents

16. US Department of the Air Force. Automatic Data

Processing (ADP) Security Policy, Procedures, and Responsibilities. AFR 205-16. Washington, DC: Government Printing Office, 1 August 1984.

17. US Department of the Air Force. COMSEC User's Guide. AFR 56-10. Washington, DC: Government Printing Office, 28 July 1986.

18. US Department of the Air Force. Communications Security (COMSEC) Duties and Responsibilities. AFR 56-11. Washington, DC: Government Printing Office, 28 July 1986.

19. US Department of the Air Force. Communications Security Policies, Procedures, and Instructions. AFR 56-50. Washington, DC: Government Printing Office, 20 July 1985.

20. US Department of the Air Force. Industrial Security Regulation. AFR 205-4. Washington, DC: Government Printing Office, 23 July 1985.

21. US Department of the Air Force. Information Security Program Regulation. AFR 205-1. Washington, DC: Government Printing Office, 7 December 1982.

22. US Department of the Air Force. Information Systems Security. AFR 700-10. Washington, DC: Government Printing Office, 15 March 1985.

23. US Department of the Air Force. Operations Security. AFR 55-30. Washington, DC: Government Printing Office, 11 April 1983.

24. US Department of the Air Force. Technical Surveillance Countermeasures (TSCM) Program. AFR 207-14. Washington, DC: Government Printing Office, 14 September 1984.

25. US Department of the Air Force. USAF Communications Security (COMSEC): A Guide for Initial and Recurring Training. AFP 56-15. Washington, DC: Government Printing Office, 28 July 1986.

26. US Department of the Air Force. USAF Personnel Security Program. AFR 205-32. Washington, DC: Government Printing Office, 26 November 1982.

END

5-87

DTIC