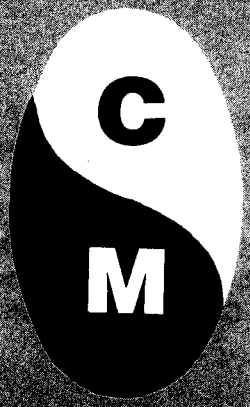
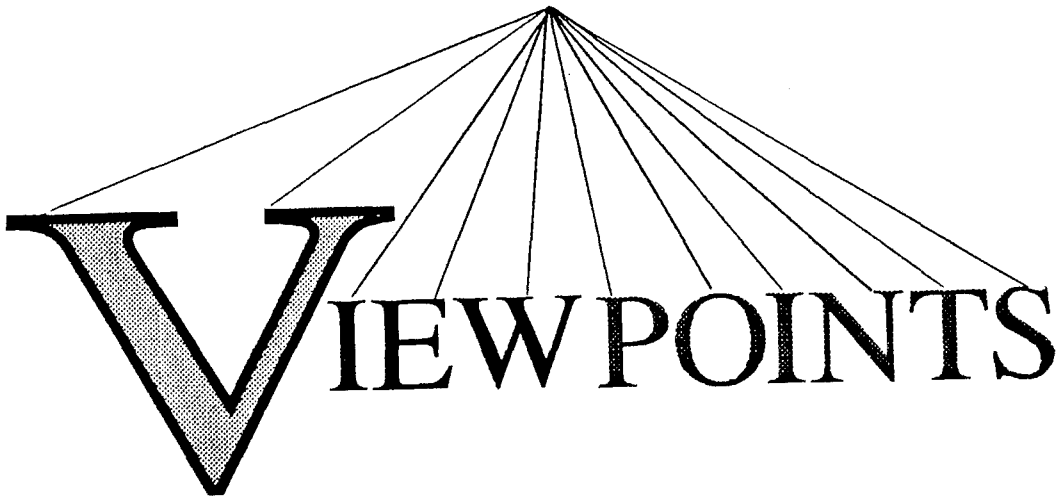


A PUBLICATION of the NATIONAL
CLASSIFICATION MANAGEMENT SOCIETY
VOLUME II, 1992

ISSN-0009-8434

Published by the National Classification Management Society. Mailing address: Executive Secretary, NCMS, 6116 Roseland Drive, Rockville, Maryland 20852. Editor of this volume: Raymond P. Schmidt. Editorial Review Board: Carol A. Thomas, LOGICON, Incorporated; Joseph A. Grau, Department of Defense Security Institute; James H. Mathena, Martin Marietta Corporation. Board of Directors Publications Oversight: David E. Whitman. Publication Coordinator and Publisher: Eugene J. Suto. The information contained in this periodical and presented by the several authors does not necessarily represent the views of their organizations or the National Classification Management Society.

Copyright © 1992 National Classification Management Society.



PURPOSE

The purposes of the National Classification Management Society are:

- To advance the profession of Security Classification Management.
- To foster the highest qualities of professional excellence among its members.
- To provide a forum for the free exchange of views and information on the methods, practices, and procedures for managing security classification programs and related information security programs.

Members are encouraged to submit articles, think pieces, scholarly studies, and letters about any aspect of classification management and information security. All security subjects are fair game for inclusion in ***NCMS VIEWPOINTS.***

PERIODICAL OF THE NATIONAL CLASSIFICATION MANAGEMENT SOCIETY

CONTENTS

Editorial Comments

Members of NCMS pursue diverse professional disciplines. Some of us are expert in Government policy regulations or industry procedures. Others have mastered personnel security issues or physical security technology, such as safe and vault specifications. Many, of course, are highly skilled in classification management.

Nevertheless, we all share many common interests. Possibly the overriding universal concern is to detect emerging challenges that make existing security programs less effective. Our future success depends upon understanding such challenges and developing viable alternative programs. Any synthesis of contending proposals must also produce a cost-effective response that works in rapidly changing threat environments.

Every day security specialists solve problems and generate innovative solutions worthy of attention by NCMS. The exchange of tested ideas and proposed new ones is a basic purpose behind *Viewpoints*, and gives this periodical its name. In our third issue, *Viewpoints* addresses several new subjects, and revisits at least one previously discussed.

The lead article acknowledges that nothing excites our imaginations and vexes us with such persistence as computers. We have only begun to see their constructive and destructive impact on security classification and safeguarding. John McCumber makes the point that "computer security" most often means controlling access to the information being processed. His discussion slices deftly through the confusion that often envelopes computer systems. His conclusion that we need an integrated approach to information security--for both automated and non-automated data--carries significant implications for the future.

Arvin Quist explores the fundamental question whether aggregated unclassified information ever qualifies for classification. His examination of this and related issues presents a closely-reasoned argument that reaches a logical conclusion many NCMS readers support. Debates sponsored by NCMS over the past decade suggest, however, that other members hold contrasting opinions. Those interested in classification issues who have not yet seen or heard this debate will find his article stimulating reading.

Jack Tomarchio describes the steps taken in preparing legal defense of a contractor who faced a challenge to his security clearance. He illustrates industrial security program rules and procedures in a fascinating case study covering pre-trial maneuvers, courtroom strategy and tactics, and post-hearing activities. His explanation of this case illustrates the value of due process protection and the role of legal counsel in granting and revoking industrial personnel security clearances. As a point of interest, he practiced a totally different kind of law in a Reserve uniform with the Army Judge Advocate General Corps during Operation Urgent Fury in Grenada and more recently during Operation Desert Storm in Kuwait.

Maynard Anderson has contributed another unique *Viewpoints* article dealing with the National Industrial Security Program (NISP). His previous article explored reasons why the United States needs a NISP. This essay reviews actions which led to development of the NISP over the decade of the 1980s. No one can read his account without sensing the compelling need for action and the sometimes fragile early consensus on key points. Those who remember his earlier article which assessed today's security reality and advocated re-creation of security policy will recall the story of the frog in hot water. Extending that analogy, we might think of ourselves as frogs in a warming pond who survive by sending and heeding warning signals and by cooperating to build bridges around the boiling bubbles.

The last three articles mentioned include extensive notes that offer useful explanations and reference sources. In fact, each author has more to say about his subject, which simply could not be included in this space. Readers may wish to contact them about specific questions.

Kurt Haase graciously agreed to adapt his operations security (OPSEC) briefing for publication. He hopes that his willingness to share the Department of Energy Nevada Field Office experience will prompt others to write about their own programs. As he notes, nearly all Government programs with information requiring protection can employ OPSEC methodology. His article refers to "The Great Conversation" monograph published in 1991 by the Interagency OPSEC Support Staff

(IOSS) for origin of the term OPSEC. Alert readers will find the makings of another "great conversation" in his article's stated OPSEC premise: "The accumulation of several elements of unclassified information could damage national security by revealing classified information." Clearly, this would entail classification by aggregation or compilation, or, if you prefer, classification in the mosaic. Interestingly, the draft IOSS glossary avoids specifying whether or not vulnerable U.S. information is classified or unclassified, or both.

Ethel Theis brings us a fresh look at the oversight function as seen by the Information Security Oversight Office (ISOO). Two contrasting inspection philosophies are described, along with her assessment of their comparative strengths and weaknesses. The article also identifies ISOO's other responsibilities under the Presidentially-mandated information security program. It will surprise some to learn that oversight is only one of a number of major activities that draw on limited ISOO staff resources. Most important is her emphasis on the goal of agency cooperation to develop a coherent and effective program that will provide adequate protection for national security information (NSI).

Robert White writes to ask for more workable guidance to allow declassification and public release of NSI no longer deserving of protection under Executive Order (EO) 12356. His title captures the essence of our problem: It is a dilemma because either course of action requires resources that are not and probably will not be made available. The U.S. track record on downgrading and declassification is uneven, and you may wish to look at specific recommendations for improvement by Al Thomas in the first issue of *Viewpoints*.

Readers may remember that President John F. Kennedy issued EO 10964 in 1961 initiating a scheme for downgrading classified information at 3-year intervals, with declassification after 12 years, and another option that downgraded information at 12-year intervals but permitted no automatic declassification.

With EO 11652 in 1972, President Richard M. Nixon prescribed the general and advanced declassification schedules, allowing automatic downgrading at two-year intervals or downgrading and declassification by a pre-determined date. The next change came in 1978 when President Jimmy Carter instituted the provision for specifying downgrading and declassification dates and the "Review for declassification" marking that was abolished in 1982. Its replacement was "Originating Agency's Determination Required" (OADR), which all but eliminated automatic downgrading and declassification except at 30 and 50 years.

One member of the *Viewpoints* editorial review board suggested that an index to published articles would prove useful. Accepting that as an excellent proposal, it will become a long-term task for some future weekend. Meanwhile, the titles and authors of previous *Viewpoints* articles appear at the back of this issue.

A reader inquired how much time is required for completing review and publication of each article. No data have been collected, but an estimated 30 hours would not be far afield. Note that this includes reading of each article by the *Viewpoints* editorial review board, which plays an essential role in the process. And this leads to the final page of this issue where you will find a summary of NCMS requirements for submitting articles. Two of the current authors introduced a useful addition: They submitted a 5-1/4 inch floppy disk of their articles using WordPerfect software. The disk reduces typing time by a wide margin, and at least one other author has submitted a disk with his article for the next issue.

This issue also marks a change of the watch in oversight by the NCMS Board of Directors. A special thanks and best wishes to Ms. Peggi Parks, and welcome aboard to Mr. Dave Whitman. Finally, an expression of appreciation to those who have taken the time to submit an article for *Viewpoints*. Everyone is invited to write at least one publishable essay, letter, or similar piece.

Raymond P. Schmidt

ALMOST EVERYTHING YOU NEED TO KNOW ABOUT COMPUTER SECURITY. . . but didn't know whom to ask!

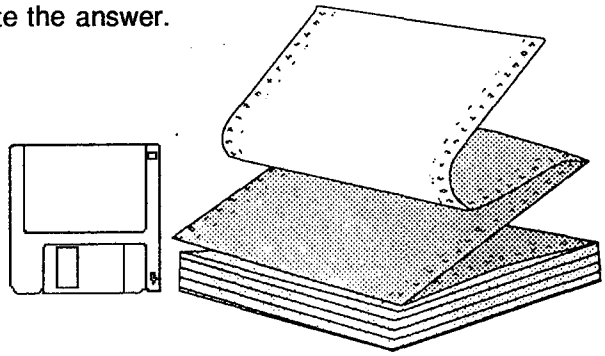
John R. McCumber*

Was it the Michelangelo virus? Perhaps it was something earlier, like the Internet worm. Or maybe you had a seemingly inconsequential hacking incident which has become an office legend. Whatever the reason, your management was prompted to ask you about the state of computer security within your organization. Usually the question asked is simple: "Just how vulnerable are we?"

You figure this cannot be too difficult to answer. All you have to do is call the computer lab for the needed assurances to placate the boss. After a tedious discussion, the operations supervisor suggests you get the "real skinny" from the technical guru. Your in-house computer expert happily provides you with jargon-rich details and system architectures which resemble instructions from a Radio Shack do-it-yourself kit. You begin to wonder whether anybody has a correct answer which management can understand!

To find a good answer, you must ask a good question. When you ask about computer security, you may already be using a misnomer. In actuality, you are not really concerned about the security of the *computer* other than the physical protection of those pieces of equipment. The real asset is the *information* which is processed, stored, and transmitted by the computer. The machine is only a mechanism for handling your information. Your concern stems from the threat of abuse or misuse of this information; in short, the consequences of *not* protecting your information. Thus the correct question is: "What are we doing to insure that our information resources are not maliciously or unintentionally delayed, destroyed, disclosed, or modified?" The next logical question is: "Have we intelligently weighed the risks and potential consequences?"

Here is what you need to know to help evaluate the answer.



INFORMATION IS AN ASSET

For all organizations, information is a vital corporate asset. Sometimes we may not comprehend its full value. For an easy analogy, consider the cash which you have in your wallet. You will certainly agree that cash is a personal asset. If someone exploits your cash assets, you will undoubtedly find out when you notice it missing. What is significant is the mental concept you have of the missing money. You don't bemoan the loss of the actual currency; the bills have little intrinsic significance. Instead, you think of it as the luncheon you now cannot attend or the lost tank of gas. You can comprehend the full asset value of the money as a function of its ability to maximize pleasure or minimize pain.

It is sometimes difficult to ascribe the same characteristics to information. Most often we think of it in relation only to its intrinsic value. You can get a sense of its value by looking at extremely sensitive information. Your organization would probably be devastated if its most closely-guarded information was exploited. Can you imagine the consequences if contract bids are leaked or mili-

The author expresses appreciation to Dr. Lynn Fischer of the DOD Security Institute for his asssistance in preparing a previous article that was used extensively in writing this piece.

tary secrets are disclosed? This mindset will allow you to begin to determine its value as an asset. Other metrics used to judge its value include the cost to recreate the data, lost opportunities, and denial of service.

The "exploitation value" of your information must remain a key component of any risk analysis. It will always be the sensitivity level of the *data*, not the applications or "system," that will determine the security measures which are necessary.

Associated with the concept of information value is the formal classification of Government information. One of the more inane distinctions I have dealt with lately is the very fuzzy line which separates unclassified from unclassified-but-sensitive information. As in the case of money, it *all* has value--whether it is a penny or a thousand dollar bill. To carry the analogy farther, consider any other form of currency or trade. All have value--the key is determining for whom!

I believe all official unclassified information must be considered sensitive and protected accordingly. This simple preventive measure would eliminate unnecessary and illogical distinctions *within* security classifications. I don't believe the government or any other community of interest produces, uses, and maintains data for which they wouldn't want (at the very least) to insure a degree of integrity and availability. These security attributes are necessary even if secrecy (classification) is not required.

"...all [information] has value--whether it is a penny or a thousand dollar bill....the key is determining for whom!"

THE CONSEQUENCES OF POOR SECURITY

Information's asset value is sometimes determined by using risk assessment methodologies. Before any good risk assessment can be accomplished, there must be some realistic evaluation of potential threats. Ultimately, this is a matter of predicting potential consequences of *not* protecting the information. These consequences are the basis for any decisions you will need to make on the nature and scope of available security measures. Basically, if it is cheaper to recover from the exploitation then to prevent its occurrence, then securing the data is not the most cost-effective approach. In short, some minimum set of security controls is necessary for all information assets.

Potential negative consequences are easy to categorize. I use the acronym D3M: destroy, delay, disclose, and modify. Destruction of data is fairly straightforward. Delay could also be termed denial of service; it describes any unacceptable state where the data are not available exactly when needed. Disclosure is potentially a much more sinister problem. As I implied earlier, information can be exploited without your knowledge and consent. Modification is possibly the most dangerous of all conditions. What if you were acting upon information you deemed reliable only to make grave errors? One need look no farther than the tragic destruction of a civilian airliner by a U.S. warship. The sensor systems all appeared to have functioned correctly; however, a proper decision became a nightmare when the automated systems portrayed a situation different from reality.

I have a friend at the IRS who looks at the risk analysis problem this way: "Detect what you cannot prevent, and prevent what you can't detect." I like this maxim because it points out there is no "complete" technology solution for the protection of information assets. However, it also tends to imply that it is necessary to guard against all eventualities. This is simply overkill.

A recently-published Government computer systems policy called for the most stringent security mechanisms possible because these mechanisms "provide the most security features that can currently be expressed." No other mention was made of the nature of the information or its sensitivity. Equally amazing was a document I reviewed which said administrative and word-processing systems did not need any security even though the data which they processed was highly-sensitive. Apparently the author felt the application--and not the data--dictated the security requirements. The information and the policy which dictates how it is handled are the only criteria for determining the mechanisms necessary for appropriate protection.

IT IS A SECURITY PROBLEM

Computer (or information systems) security is a *security* problem, not a computer problem. Many organizations mistakenly throw the "computer security problem" in the lap of ADP management.

Although computer systems personnel are responsible for implementing most of the technical security measures, security is not really in their best interests. In fact, security only makes their job more difficult. Data centers are normally rated by their ability to make the data available. Since it is not actually "their data," they are not often held accountable for exploited, missing, or incorrect information. Oversight for computer security implementation and monitoring must reside with security professionals.

Because it is a security problem, it must be addressed as any other security problem. The appropriate preventive security measures must be implemented to protect this sensitive asset and, when security breaches are discovered, remedial action must be swift and decisive.

INFORMATION HAS THREE STATES

If we are to place emphasis on the information (data*) as opposed to the computer/telecommunications system or applications, then we must be able to define and understand the nature of information. Just as water takes the form of liquid, solid, or vapor, so it is that, at any given moment, information exists in one of three conditions: It is being either processed, transmitted or stored. The three states exist irrespective of the medium on which information resides. For example, you can store the same information on a computer fixed disk as on paper.

"Information exists in one of three conditions: It is being either processed, transmitted, or stored. ...[And information possesses] three critical characteristics: ... confidentiality, integrity, and availability."

The distinction among the three states is fundamental to understanding the security approach I offer for evaluating data security programs. For example, encryption can be used to protect information while it is transferred through a computer network and even while it is stored in magnetic media. However, the information must be available in plaintext in order for the computer or user to perform the processing function. The processing function requires specific security controls.

SECURITY DICTATES THREE CRITICAL CHARACTERISTICS

Just as information can exist in three states, information systems security must be aimed at ensuring three critical *characteristics of the same information:* confidentiality, integrity, and availability. These attributes of information represent the full spectrum of security concerns in an automated environment--actually in any environment. Neither the state nor the medium on which the information exists is the primary consideration. When information is needed to make a decision, the end user may not be aware of how many times the information has changed from one state to another or on how many different media it has been stored. The primary concern will be the *characteristics of the information* which together maintain its value to the user. These are worth protecting and, therefore, constitute the security-relevant qualities of the information.

In non-automated environments, the issue of confidentiality seems to hold overriding importance. Nevertheless, even in a paperbound workplace, information integrity and availability are essential. A classified document is of no value unless it is accessible to the right people, and can be positively lethal if someone has falsified the information in that document. So when evaluating the security effectiveness in the automated workplace, we must think of potential threats to information not only in terms of theft and misuse, but also with regard to intentional and unintentional corruption, or even total destruction of data files.

SECURITY MEASURES

Security measures can also be conveniently categorized in three distinct classes: technology, policy and practice, and education, training and awareness (see Figure 1). Together, they can be thought of as preventive devices and methods to prevent the loss, compromise and destruction of our valuable information. (As preventive mechanisms or methods, it may be argued that the use of the term "countermeasure" is more in line with contemporary parlance.)

**I use the words data and information interchangeably because, in automated systems, numbers and alphabetic characters are stored and processed in the same way.*

Layers of Security Measures by Information States

	TRANSMISSION	STORAGE	PROCESSING
TECHNOLOGY	STU-III Data encryption devices Codc Parity Error checks	Access codes Password controls Physical safeguards Intrusion protection SCIF construction	Trusted systems (NSA) User recognition systems Multi-level processing Error traps Anti-virus software
POLICY/ PRACTICE	Data encryption standards Personnel security	User access policy User authorization Approved systems (DIS) Physical safeguards Approved storage Personal Security	Access control policy Approved systems (DIS) Audit trails Personnel security
EDUCATION TRAINING AWARENESS	COMSEC training STU-III indoctrination	Security indoctrination Physical protection training	Security indoctrination Security education Computer security briefings

Figure 1

For our purposes, we can define technology as any physical device or technique which is specifically employed to maintain the critical information characteristics through any of the information states. Technology can be implemented in the form of hardware or software. It could be a biometric device, cryptographic module, or security-enhanced operating system.

A purely technological perspective creates its own problems, however. Usually, organizations are built around specific tasks (*i.e.* a functional grouping). The advent of computer technology created the need for a specialized group of employees to accommodate the machines which would process, store, and transmit much of our vital information. In other words, the organization was adapted to suit the evolving technology. Was this wrong? Not necessarily; however, it created the impression that technology exists for technology's sake. In reality, telecommunications and computer systems are simply among the many media on which information can exist in one of the three states.

Policy and practice, as in any security discipline, are significant aspects of preventive protection. A security policy is simply the rules that determine whether a person can have access to a given category or piece of information. A recent study has shown that 75% of Federal agencies do not have a policy for the protection of information on PC- and workstation-based information systems. These would establish rules about user access control; physical storage requirements for media, software, and equipment; audit trails; and electronic transmission. Why is policy such a neglected security measure when it comes to automated systems?

Because of an exaggerated reliance on technology, it is easy to think of security solutions as devices or add-on packages for existing information systems. Some security professionals are guilty of waiting for technology to solve that which is not solely a technological problem. And we are likewise guilty of pouring enormous resources into high-tech countermeasures as if they were a panacea. Policy development is the single most critical step you must take to begin the process of protecting information assets. These policies must be enforced by regulations that have teeth. There must be predictable consequences when violations are discovered.

Technology and policy/practice represent the design and application of a security-enhanced information system. Education, training and awareness represent the *understanding* necessary to protect information. Although an integral aspect of the preceding two security measures, education must be considered separately because it is capable of standing alone as a significant security measure.

"[This approach integrates] conventional security practices and measures...[with those of] automated information systems."

THE BIG PICTURE

I have now outlined the ingredients for a complete understanding of the information systems security arena. By identifying the various states of information as it flows though a system, whether automated or manual, you can determine if its critical information characteristics are being maintained. You can determine if any security measures are already in place, what they protect (which characteristics), and what is missing. By using this procedure as the foundation for a top-down approach to information systems security, one can begin to grasp the full scope of possible security measures. Even if there is no specific control available to counter a vulnerability, the knowledge that a vulnerability exists (and where) is a significant improvement over blind ignorance. In this case, the applied security measure would be one of awareness, resulting in changes to human behavior (*e.g.*. greater alertness).

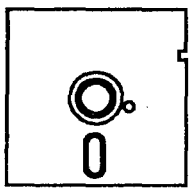
A major implication of this approach is the integration of conventional security practices and measures, and those which belong to the automated information systems environment. In reality, they should be seen as belonging to one integrated system having both automated and non-automated components.

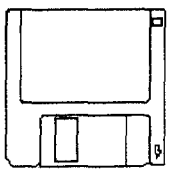
Now you can feel comfortable answering those tough questions about computer security. After showing management how computer security is just one aspect of your organization's overall information security plan, you pass out copies of the organizational information security policy. You then

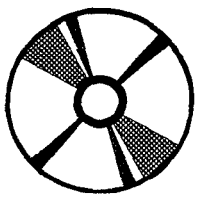
show how information changes states as it flows through the organization. You then explain what measures are employed to ensure the confidentiality, integrity and availability of these assets. You, as a security or information professional, have a seamless program which takes a comprehensive approach to key threats in the post-Cold War environment.

As information professionals, we should seriously consider eliminating confusing and nebulous distinctions within unclassified information. *All* information has value and reveals something about our organizational posture. We should be concentrating on the dynamic threat to our vital information assets. In 1988, the Department of Justice found that the average bank robber made off with $6100 whereas the average computer criminal was able to obtain $883,279 in assets. It is obvious to see that a bank spends much to protect its monetary assets. Comparatively, are we expending enough effort and resources to protect our information? After all, it is our single largest and most vital national asset.

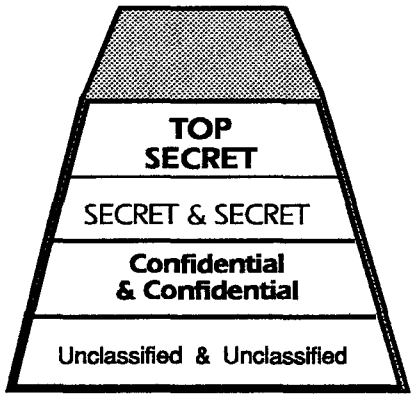
John R. McCumber, a Captain in the United States Air Force, serves as action officer in the Information Security Division of the Directorate for Command, Control, Communications, and Computers (J-6), Joint Chiefs of Staff.







WARNING
These media can be hazardous to your security.



CLASSIFICATION OF COMPILATIONS OF INFORMATION

Arvin S. Quist

INTRODUCTION

Information is given a security classification when its unauthorized disclosure reasonably could be expected to cause damage to our national security. Classification of information results in unavoidable costs. Because of those classification costs, it is important to classify only that information which truly warrants protection *and* which can be kept from an adversary.

It might seem obvious that compilations of *unclassified* items of information should not be classified. When an individual item of information is unclassified, then a decision has been made that this item of information does not need the special kind of protection prescribed for classified information, that the information does not need to be kept from an adversary for national security reasons. If individual items of information are not protected from an adversary, then an adversary can obtain and compile them. Consequently, it would seem that a compilation of unclassified information items should not be classified when an adversary can independently prepare the same compilation. However, there are many instances where compilations of previously unclassified information have been classified.

For example, compilations of unclassified titles or unclassified summaries of classified Department of Defense (DoD) projects have sometimes been determined to be classified because "trends" of classified DoD research and development are thereby revealed. If "trends" of classified research warrant classification and those trends are revealed by compiling unclassified titles or abstracts of the classified projects, then the titles or abstracts of individual projects should be classified so that the trends are not revealed. Otherwise, there is no way to ensure that an adversary could not obtain the unclassified titles or abstracts and thereby detect those trends.

It is important, for two major reasons, not to classify compilations of unclassified information. The first reason is to avoid classification costs when the "classified" information cannot be protected--when an adversary can obtain that information by independent, nonespionage efforts. The second reason is to maintain the credibility of the classification program, an important aspect of successful classification policy. It is difficult to maintain classification credibility, to ensure that information which truly warrants protection for national security reasons is protected, when information that obviously can not be protected is nevertheless assigned a classification category and level.

Classification specialists do not agree that compilations of unclassified information should be unclassified in all circumstances. The main purpose of this paper is to discuss comprehensively the classification of compilations of unclassified information. A related topic is whether a compilation of many items of information classified at one level (*e.g.*, Confidential) can sometimes be classified at a higher level (*e.g.*, Secret). Finally, this paper proposes certain rules for use when considering the classification of compilations of information.

It should be noted that the classification of information because of its *association* with other information is a subject different from the classification of compilations of information. There is no doubt that information which is unclassified *per se* may be classified when it is associated with certain other information (*e.g.*, materials or components

that are unclassified *per se* may be classified when associated with a classified project or hardware item). This discussion about classification of compiled information assumes that there is no association of information within the compilations that would make the compilations classified.

DEFINITION OF THE TERM COMPILATION

Many of the differences of opinion about the classification of compilations of unclassified information probably result from ambiguities about the meaning of the term compilation. Some of those differences can therefore be eliminated by defining the word. In this paper, a compilation is defined as an orderly arrangement of preexisting materials (facts, statistics) gathered from many sources into one document.

To further aid in the discussion of classification of compilations, it is useful to establish two major types of compilations: (1) compilations that have had no substantive value (information) added by the compiler (true compilations), and (2) compilations to which substantive value has been added by the compiler. Compilations of the first type contain only information that was present in the individual items of information that constitute the compilation. Compilations of the second type contain substantive information added by the compiler [*e.g.*, the compiler used expert judgment to select certain information for the compilation, or the compiler added new substantive information (*e.g.*, critical comments) to available information]. The same classification rule does not apply to both types of compilations. The next two sections consider both types.

COMPILATIONS OF UNCLASSIFIED INFORMATION WITH NO SUBSTANTIVE VALUE ADDED

Description

Compilations of information to which no *substantive* value (information) was added by the compiler are merely compilations of existing information arranged in an orderly fashion. These are true compilations. The compiler has not used judgment to select or discard items of information and has not otherwise added information based on subject-matter expertise--*the compiler has not added any substantive value to the information selected for the compilation.* No information was added by the compiler that was not present in the individual items of information that constitute the compilation. The total store of knowledge concerning the subject matter of the compilation has not been increased by the compiler.

Compilations of this type may be prepared by someone not having expertise in the subject matter of the compilation. One example of such a compilation would be a township map that shows the location, size, and ownership of parcels of land as obtained from public records. Another example would be data on the highway mileage between all the cities in a state, prepared from city, county, or state highway maps available to the public. A third example would be a directory of names and addresses of residents of a city, in alphabetical order by name, produced from an unordered file containing those names and addresses. A final example would be a list of all the titles of reports prepared for a specific Governmental agency during a fiscal year and sent to the National Technical Information Service (NTIS), where the individual report titles were obtained from NTIS publications or the NTIS data base. These compilations could be prepared by clerical personnel, as contrasted to surveyors, tax assessors, or technical experts. They are useful, but their value arises because the compiler has gathered together all the pertinent information on a subject and arranged it in a *form* that enables convenient use of that information.

Classification of Compilations with No Substantive Value Added

Proposed Classification Rule and Its Rationale. Compilations of unclassified information to which the compiler has added no substantive value (no substantive information) should not be classified. This conclusion is based on a fundamental principle of classification--that classified information cannot be completely subdivided into separate, unclassified components. The Department of Energy (DOE) has stated this principle as follows:

> *Information that is classified under the Atomic Energy Act must not be so subdivided that all its components (including contextual information) are unclassified.*

This is sometimes called the *keystone principle of classification.* It may be visualized by considering a classified photograph or drawing that has been subdivided into many components (*e.g.*, pieces of a puzzle), each of which reveals an item of information. According to this principle, not all of those pieces can be unclassified if the entire

entity is classified. One or more key pieces must be classified so that the entire picture cannot be obtained when all the unclassified pieces are assembled. Thus, if individual items of information are truly unclassified (*i.e.*, if no classification error has been made), then assemblies (compilations) of those items cannot reveal classified information.

A proposed rule for classifying compilations of unclassified information where no substantive value has been added by the compiler, and which is a corollary to the basic DOE classification principle, is as follows:

> *If all components (including contextual information) of a compilation are unclassified, and no substantive information (value) has been added by the compiler, then the compilation should not be classified.*

The essence of this rule was set forth over thirty years ago by the Atomic Energy Commission (AEC) in a 1958 AEC *Monthly Classification Bulletin*:

> *A compilation of unclassified information is unclassified. Therefore, if an area of information has an overall classification, some, if not all, of the data which makes up this area must be classified.*[1]

The Nuclear Regulatory Commission has published similar guidance for the classification of compilations:

> *Compilations of unclassified information are generally considered to be unclassified unless some additional factor is added in the process of compilation. For example: (a) The fact that the information is complete for its intended purposes may be classified; or (b) the fact that compiled information represents an official evaluation may be classified.*[2]

This proposed rule for the classification of compilations of unclassified information is consistent with a requirement of Executive Order (EO) 12356 for the classification of information: Only information that is "owned by, produced by or for, or is under the control of the United States Government" can be classified as National Security Information.[3] If the individual items of information that constitute a compilation are unclassified, then they are not under the control of the Government to the extent required by security procedures for protecting classified information (*e.g.*, the documents containing the items of information are not kept in secure repositories while they are unattended, they are not marked so as to be kept from unauthorized persons). If none of the items of information in a compilation is controlled by the Government *to the extent required for classified information*, then the compilation may not be classified as National Security Information.

The conclusion that one should not classify compilations of unclassified information with no substantive value added by the compiler is also supported by another EO 12356 requirement: Information may be classified only if its unauthorized disclosure reasonably could be expected to cause damage to the national security.[4] That order defines three levels of classification--Confidential (C), Secret (S), and Top Secret (TS)--that correspond to three levels of damage: damage, serious damage, and extremely grave damage.[5] Providing for three different damage levels indicates that damage quantification is expected. If the unauthorized release of an item of information reasonably could be expected to cause damage, then the information is considered Confidential information.[6] Let us assume that the damage caused by the release of an item of Confidential information would be "1" on an arbitrary scale of damage. (For Secret and Top Secret information, the damage value would be greater.) The release of an unclassified item of information would cause no (zero) damage to our national security (by definition of what constitutes classified information). Therefore, no matter how many items of unclassified information are compiled (added together), the sum of the damages caused by their release would still be zero and the compilation should not be classified.

EO 12065, the immediate predecessor to EO 12356, included a statement that "references to classified documents that do not disclose classified information may not be classified or used as a basis for classification."[7] This would seem to indicate that a compilation of unclassified titles of classified documents would not have been considered classified under EO 12065.

Trade Secret Law and the Proposed Classification Rule. There are many similarities between the classification and protection of national defense and foreign relations information (state secrets) and the identification and protection of trade secrets. Therefore, it is useful to examine

the extent to which compilations of information important to businesses are protected under trade secret law to help determine whether similar compilations of Government information should be classified.

A compilation of unclassified technical information is analogous to a combination of a series of widely known industrial processes, such as common shop practices. A combination of common shop practices will not be considered a trade secret unless the combination is unique, that is, unless something substantive or some special insight was added when that combination was developed.[8] "A trade secret can exist in a combination of characteristics and components, each of which, by itself, is in the public domain, but the unified process, design and operation which is an *unique combination*, affords a competitive advantage, and is a protectable secret (emphasis added)."[9] The rule that a compilation of unclassified information, which has had no substantive value added by the compiler, should not be classified is therefore consistent with trade secret law which requires that a combination of publicly available information have substantive value added before that combination (compilation) is a trade secret.

Copyright Law and the Proposed Classification Rule. Classification and copyright protection are also somewhat analogous, since classification protects information from unauthorized disclosure to adversaries and copyright protects materials from unauthorized use by a competitor.

Copyright protection is provided by a U.S. statute to original works of authorship,[10] including compilations.[11] A compilation is defined as "a work formed by the collection and assembling of preexisting materials or data that are selected, coordinated, or arranged in such a way that the resulting work as a whole constitutes an original work of authorship."[12] An important question concerning copyrightability of compilations of publicly available (*i.e.*, unclassified) information is what constitutes an original work of authorship. Originality, with respect to compilations and copyright law, may be achieved by arranging facts in a systematic fashion[13,14] or by adding material to facts[15] (*e.g.*, by adding substantive value). It is the *selection* (*e.g.*, names in a social register, stocks in the Dow Jones listings[16]) or *arrangement* of facts that is copyrightable, not the facts themselves.[17,18,19] The copyrighting of a compilation does not affect the status of the materials from which the compilation was made and which are in the public domain.[20,21]

Copyright law requires subjective judgment to be used by a compiler of publicly available information before that compilation can be copyrighted. Therefore, the rule that compilations of unclassified information, without substantive value added by the compiler, cannot be classified is consistent with copyright law, which protects only compilations that derive their value from the expert judgment or originality used by the compiler in preparing the compilation.

Judicial Decisions Supporting the Proposed Classification Rule. A 1976 Federal District Court case involved a compilation of *unclassified* titles of technical reports on research projects under way for the Department of Defense (DoD). Some of the technical *reports* were classified but their *titles* were unclassified. Compilations of those unclassified report titles (*Technical Abstract Bulletin Indexes*) had been issued as unclassified for several years until DoD began classifying them because the compilations were believed to reveal research directions and trends of national defense importance. A Freedom of Information Act (FOIA) request was made for the classified document (the compilation of unclassified titles); the request was refused by DoD; and the matter was litigated. A Federal District Court ordered DoD to release all the unclassified entries in the document.[22] Since that meant that all the report titles in the compilation would have to be released, DoD released the entire document as an unclassified document.[23] Although the court did not address the question of whether the compilation was improperly classified, the practical effect of its decision was that the compilation itself was an unclassified document. This result is consistent with the proposed classification rule.

Views Not Supporting the Proposed Classification Rule. The proposed rule that compilations of unclassified information with no substantive value added by the compiler should not be classified is not unanimously accepted. An opposing view believes that compiled items of unclassified information should sometimes be classified. Sometimes a compilation is said to be classified when it contains a nearly complete list of certain items of information which are unclassified when they are isolated items of information. For example, classification guides dealing with communications security (COMSEC) matters have included guidance to the effect that individual inventory reports of certain COMSEC materials are unclassified, but reports that contain a substantially complete listing of those

that contain a substantially complete listing of those materials at a facility are classified. As discussed earlier, it does not seem effective to classify such a listing because an adversary could obtain the same information from the unclassified individual reports.

Sometimes a compilation is said to provide information not present in the absence of the compilation--to make evident some classified information not revealed by the individual items of information in the compilation when isolated from each other. This would be new information that is perceptible because of the compilation.[23,24,25] Under that situation, some classifiers believe that the compilation should be classified. This view receives some support from the DoD. The DoD has stated that normally a compilation of unclassified items should not be classified, but that "in unusual circumstances, classification may be required if the combination of unclassified items of information provides an added factor that warrants classification.[26] Individually unclassified items that become classified when associated with one another have been cited as an example of this added factor.[27] However, as was mentioned earlier, classification because of associations is a separate topic from classification of compilations.

In situations such as those described in the preceding paragraph where classified information is alleged to have been obtained via compilations of unclassified information, it is likely that, in fact, a classification error was made. That is, the classification guidance applicable to the situation was not comprehensive. The guidance did not include all the inferences that an expert could draw from the information under consideration for classification. Those inferences should include those associations which could be made when combining the information under consideration for classification with all existing unclassified information. A classification determination must always be based on the assumption that any person who receives the information under consideration for classification is (1) highly qualified in that particular field of technology and (2) thoroughly familiar with all related information that has already been issued as unclassified. Thus, when a compilation of unclassified information is said to reveal new, classified information, it is probable that the existing classification guidance should be revised to classify one or more of the individual items of information that lead to the revelation of this new information.

EO 12356 is said by some to provide a basis for classification of a compilation of unclassified bits of information. Section 1.3(b) of that EO states that before information can be classified, an original classifier must determine "that its unauthorized disclosure, *either by itself or in the context of other information*, reasonably could be expected to cause damage to the national security"[28] (emphasis added). The phrase "either by itself or in the context of other information," which was not present in the immediately preceding EO, is said to be recognition of the compilation theory of classification.[29] A better interpretation of Sect. 1.3(b) would be that "in the context of other information" refers to *associations* of information, rather than *compilations*. As stated previously, it is a long-standing classification principle that associations of information may be classified when the association reveals classified information.

Judicial Decisions Not Supporting the Proposed Classification Rule. In a 1982 case [*Taylor v. Department of The Army*, 684 F.2d 99 (D.C. Cir., 1982)], a newspaper reporter had requested, under the FOIA, the Army's numerical ratings for the four measured resource area ratings (MRARs) for all 168 major combat units of the Army. At the time of the request, an Army regulation unequivocally stated that the MRARs for single units were unclassified. However, the Army interpreted its regulation to mean that the raw data were unclassified, not the MRARs, and refused to provide the MRARs because they were considered by the Army to be classified. Subsequently, a Federal District Court directed the Army to release the information.

The District Court held that the requested MRARs should be released because an Army regulation concerning the MRARs specifically stated that the MRARs for a single unit were unclassified. Although the Army argued that the information should be denied because it was a compilation of unclassified information with an added factor and was therefore classified under another Army regulation, the District Court rejected this argument. The District Court said that requesters could avoid the compilation problem by having different individuals submit FOIA requests, one-by-one, for the ratings of the different units. The District Court was not convinced otherwise by an Army affidavit that stated that an attempt to get the MRARs one-by-one "would have been uncovered at a very early stage" and that those individual MRARs would not have been provided by the Army.[30]

The Army appealed that decision to a Circuit Court, which reversed the District Court decision. The Circuit Court accepted the Army's argument that the information was classified, relying on affidavits from three Army generals which stated that this information had always been considered as classified by the Army (the applicable Army regulation had been promulgated about 18 years earlier). The Court stated that the Army should be accorded great deference in construing its own regulation.[31] The Circuit Court also may have been influenced by the Army's action, taken immediately after the Army first denied the request for the MRARs, to change its regulation to specifically classify the MRARs for a single unit as Confidential. The Court also accepted the Army's argument (supported by the affidavits of two generals) that the requested information was a compilation of unclassified information with an added factor of sensitivity and was classifiable under another Army regulation.

Although the Court in *Taylor v. Department of the Army* accepted the argument that compilations of unclassified information could be classified, the Court's decision appears to rely mostly on the Army's affidavits that the Army had always considered the requested information to be classified *and* on the fact that the Army had immediately revised its regulations to explicitly declare that information to be classified. Also, the Court stated that the requested compilation had an added factor.[32] An added factor such as substantive information provides a basis other than the compilation theory by which a compilation can be classified (see the following section). Therefore, upon detailed analysis, *Taylor v. Department of the Army* does not appear to be inconsistent with the proposed rule which forbids the classification of compilations of unclassified information with no substantive information (value) added.

A 1987 U.S. Circuit Court decision also appears not to support the proposed rule. This decision, *American Friends Service Committee v. Department of Defense*,[33] concerned DoD's Technical Abstract Bulletins (TABs). The DoD used the compilation theory to classify those TABs. A U.S. District Court decided, via summary judgment, that the TABs were properly classified. The Circuit Court to which the District Court's decision was appealed also accepted the compilation theory. However, the Circuit Court's discussion of the compilation theory described it as classification in context,[34] which, as mentioned earlier, has long been accepted as a legitimate reason for classification. Although the DoD's compilation theory was accepted, the Circuit Court vacated the District Court decision and remanded the case for several findings of fact. One question to be answered on remand was whether a significant number of the TAB entries were also published in the NTIS catalog, which is available at public libraries.[35] By the time the case was considered again by the District Court, the DoD was no longer publishing the TABs but was publishing another document which omitted certain information contained in the TABs. Therefore, future information of the type requested by plaintiff American Friends Service Committee was available. Since this action by DoD appeared to demonstrate that the information contained in the previous TABs was segregable, the plaintiff asked that DoD provide the requested information from those TABs. However, the District Court denied that request.

COMPILATIONS OF UNCLASSIFIED INFORMATION WITH SUBSTANTIVE VALUE ADDED

Description

A compilation of information with substantive value (information) added by the compiler is a compilation prepared by a compiler whose expertise in the subject matter of the compilation was necessary to prepare that compilation. This type of compilation is significantly different from a mere compilation of information. The compiler's expert judgment may have been used to select certain information (*e.g.*, the "reliable" information) for the compilation from a broader array of available information. Technical handbooks (*e.g.*, the *Handbook of Chemistry and Physics*[36]) are examples of such compilations. Substantive value is also added when a compiler includes all relevant information and then provides critical comments (expert evaluations) on the accuracy or reliability of that information. Scientific and technical review articles are examples of this type of evaluation. This latter substantive value added compilation is frequently designated a review, a critique, an analysis, an evaluation, or some other similar term.

Classification of Compilations with Substantive Value Added

If a compiler has added some information of substantive value to a compilation of unclassified information, then the resulting compilation should be classified *(1) if the added information is consid-*

ered to be classified per se, (2) if the added information is classified because of association with the preexisting information, or (3) if the preexisting information is classified when associated with the added information. This rule is not a new rule proposed for the classification of compilations of unclassified information with substantive value added. Rather, it is a principle by which all documents are evaluated to determine the security classification of information.

Judicial Decisions on Classification of Compilations with Value Added

A 1978 Federal District Court case involved a request for the release of a compilation of the number and exact titles of National Security Study Memoranda and National Security Divisional Memoranda issued between January 20, 1969, and the date of the request.[37] The National Security Council (NSC) compiled that information but then refused to release this compilation because it contained classified information (*i.e.*, the compilation included classified and unclassified titles and also gave the chronological sequence in which the individual reports were produced). The requester then asked for a compilation of the unclassified titles, and the NSC again refused to release the requested information. The Staff Secretary of the NSC submitted an affidavit stating that "Access to the unclassified titles in their totality would . . . enable a foreign intelligence analyst to identify the kinds of issues of grave concern to the United States and the way in which this government reacts to world events, and also to gain unique insights into the method by which issues of this kind are identified, studied and resolved by the President."[38] Government affidavits also stated that the compilation would provide other nations "with valuable information and insight pertaining to the focus and timing of key U.S. foreign policy concerns."[39] The Court determined that the list was "reasonably classified in full, unclassified titles included,"[40] and exempted the list from release. The sequential nature of the titles on the lists may have been a major factor in the decision, since the Court said that "this decision is, however, without prejudice to any future claim by plaintiff for access to any unclassified documents now in existence, or any unclassified documents that may come into existence, which list the unclassified titles . . . in 'scrambled' sequence and in edited form."[41]

Although the titles to the reports in the compilation were unclassified, the compiler had listed those titles in chronological order and had included the dates when the reports were prepared. The Court was of the opinion that those dates added substantive information (value) to the compilation, particularly with respect to intelligence considerations. The Court therefore upheld the agency's determination that the compilation should be a classified document. This outcome is consistent with the earlier-proposed rule that compilations of unclassified information with no substantive value added by the compiler should be unclassified. It is also consistent with the general rule that courts should extend the utmost deference to opinions of an agency's experts concerning the classification of documents generated by that agency.

COMPILATIONS OF UNCLASSIFIED INFORMATION REQUIRING SUBSTANTIAL EFFORT TO COMPILE

One reason for classifying information is to make an adversary expend its own resources to get that information. A typical example of this situation is the classification of scientific or technical data that would be useful to an adversary and that the adversary could obtain by the straightforward application of its available scientific or technical resources and by well-known methods. If the data are classified, then the adversary must expend its resources to get that data, resources that might otherwise be used to harm our nation. However, because of the inherent costs associated with classifying information, normally such scientific or technical data are not classified unless *substantial* resources would be required to obtain that data. That is, the information is not classified unless publishing it would save an adversary a substantial amount of effort in acquiring that information by the adversary's own efforts.

A possible rule for the classification of compilations of information that have required substantial efforts to produce, and which would be an exception to the previously proposed rule, is as follows:

> *If a* substantial *effort was required to produce a compilation of unclassified information and* if *an adversary would expend about the same effort to independently get that information,* then *that compilation should be classified.*

There is even reasonable quantitative guidance available as to what constitutes substantial effort.

However, the substantial effort principle with respect to classifying scientific or technical data is limited to data obtained by using *scientific or technical expertise.* Even though the effort to obtain that scientific or technical data is a straightforward application of known principles, *scientific or technical expertise is necessary* to apply those principles and obtain that data. The compilations to which the possible above-mentioned rule would apply are those compilations that require *no subject-matter expertise* to produce. The two situations are not comparable. The accepted classification principle that allows classification of scientific or technical data when substantial scientific or technical effort was required to produce that data is analogous to the classification of compilations which required expertise for their production (compilations with substantive value added during their production). Therefore, there appears to be no basis to classify a compilation just because substantial effort was required to produce that compilation.

This conclusion is consistent with copyright and trade secret law. The majority view in copyright law holds that the *effort* required to obtain information for a compilation is not a factor in determining whether the result is copyrightable. Although some courts have extended copyright protection to certain types of compilations to protect the product of the compiler's industry,[42] or the compiler's effort in collecting the data,[43] theirs is a minority view. The policy of that minority line of decisions seems to be to prevent unfair use of an author's efforts, to require others to do independent research to get the benefits therefrom.[44] Trade secret law is consistent with copyright law on this matter. The effort required to develop a new arrangement of pre-existing, publicly available information is not a factor in deciding whether that arrangement is a trade secret. Therefore, a simple substantial effort exception to the proposed rule on classification of compilations of unclassified information is not supported by the majority views in copyright or trade secret law.

CLASSIFICATION LEVEL OF COMPILATIONS OF CLASSIFIED INFORMATION

The accepted rule concerning the classification of compilations of classified information is that the compilation is classified at the same level as the highest classification level of any item of information contained therein. However, consistent with sound classification principles, under certain conditions a compilation of many items of information, all of which are classified at one level (*e.g.*, Confidential), can be classified at a higher level (*e.g.*, Secret). This conclusion is based on certain classification of information requirements contained in EO 12356 as described in the following paragraph.

EO 12356 states that information may be classified only if its unauthorized disclosure reasonably could be expected to cause damage to the national security. Providing for three levels of damage (C, S, and TS) indicates quantification of that damage by a classifier. If the unauthorized release of an item of information reasonably could be expected to cause damage, then it is considered Confidential information. Let us assume that the damage caused by the release of an item of Confidential information is "1" on an arbitrary damage scale. Assume that the release of an item of Secret information causes a damage of "100" (serious damage). If the release of an item of information could cause extremely grave damage (*i.e.*, the information has been classified Top Secret), assume that a damage of "10,000" results. On that basis, the release of a compilation of l00 *different* items of Confidential information, with each item causing a damage of 1 if released, could cause an aggregate damage of 100. Therefore, a compilation of 100 or more different items of Confidential information should be classified Secret since its release could cause damage of 100 or more. The same rationale would apply to classifying as Top Secret a compilation of 100 or more different Secret items of information.

On the basis of the foregoing discussion, a possible rule for the classification level of compilations of classified information is as follows:

> *A compilation of many* different *items of information classified at one level (e.g., Confidential) should be classified at a higher level (e.g., Secret) if the total damage caused by the unauthorized release of all of these items of information would equal or exceed the damage caused by the release of one item of information classified at that higher level.*

This is, in theory, a potentially useful principle to help determine classification levels of documents. Although it is difficult to quantify damages for the unauthorized disclosure of each item of information to the extent required to apply this rule, that difficulty is not different in kind from the problems already frequently encountered by original classifi-

cation authorities or DOE Authorized Classifiers when determining whether information should be classified and, if so, at what level.

Unfortunately, there appear to be some security-related obstacles to implementing such a rule. Consider Confidential Restricted Data (CRD), which is available within the DOE on a need-to-know basis to "L"-cleared personnel, and Secret Restricted Data (SRD), which is available to "Q"-cleared personnel but not to L-cleared personnel. Consider also the above-mentioned values for individual different items of Confidential information ("1") and Secret information ("100"). Presumably, an L-cleared person could acquire, on a need-to-know basis, over 100 different CRD items of information. By the above-mentioned rule, that L-cleared person then would have knowledge of SRD information, which would not be in accord with DOE's security regulations. What would the Security Department do in such a situation? Request a Q-clearance for that employee? Give someone a security infraction for providing SRD to an L-cleared person?

Consider also two reports containing only CRD information. One contains 60 CRD items and the other contains 50 CRD items, for a total of 110 *different* CRD items of information. An L-cleared person would need only acquire those two reports to obtain information classified as SRD by the above-mentioned rule. Situations such as those mentioned in this paragraph would occur frequently if the Government adopted this rule. Obstacles cited above would cause significant problems for those who implemented it.

CONCLUSIONS

The general rule proposed for the classification of compilations of unclassified information is as follows:

> *If all components (including contextual information) of a compilation are unclassified and no substantive information (value) has been added by the compiler, then the compilation should not be classified.*

A substantial effort exception to this rule was considered and rejected as inconsistent with other classification principles and with trade secret and copyright law.

The following rule was considered for use in establishing the classification level of compilations of classified information:

> *A compilation of many* different *items of information classified at one level (e.g., Confidential) should be classified at a higher level (e.g., Secret) if the total damage caused by the unauthorized release of all of these items of information would equal or exceed the damage caused by the release of one item of information classified at that higher level.*

This rule appears sound in theory, but security-related difficulties associated with applying it to real world situations may preclude its general use.

Arvin S. Quist is Classification Officer for the Oak Ridge K-25 Site and Oak Ridge National Laboratory, which is managed by Martin Marietta Energy Systems, Inc., Oak Ridge, Tennessee for the U.S. Department of Energy.

FOOTNOTES

[1]The U.S. Atomic Energy Commission Monthly Classification Bulletin, from which this quotation was taken is (or was) classified. Therefore, a specific reference is not given.

[2] 10 CFR part 75, App. A, Introduction, §D.6.

[3] Exec. Order No. 12356, **47** Fed. Reg. 14874 (April 6, 1982), §6.1(b) and §6.1(c). Hereafter this Executive Order is cited as "EO 12356."

[4] EO 12356, Preamble.

[5] EO 12356, §1.1(a).

[6] EO 12356, §1.1(a)(3).

[7] Exec. Order No. 12065, **43** Fed. Reg. 28949 (July 3, 1978), §1-604.

[8] Imperial Chemical Industries v. National Distillers and Chemical Corp., 342 F.2d 737 (2nd Cir., 1965); M. F. Jager, *Trade Secret Law*, Clark Boardman Co., Ltd., New York, 1988, pp. 5-53, 5-54, and citations therein.

[9] Imperial Chemical Industries v. National Distillers and Chemical Corp., 342 F.2d 737, 742 (2nd Cir., 1965).

[10] 17 U.S.C. §102(a) (1982).

[11] 17 U.S.C. §103 (1982).

[12] 17 U.S.C. §101 (1982).

[13] T. M. Gerritzen, "Copyrighting the Book of Numbers - Protecting the Compiler: West Publishing Co. v. Mead Data Central, Inc.," *Creighton Univ. L. Rev.*, **20**, 1133-1166 (1987), p. 1163, n.353. Hereafter cited as "Gerritzen."

[14] Gerritzen, p. 1163.

[15] Gerritzen, p. 1163, n. 349.

[16] D. E. Shipley and J. S. Hay, "Protecting Research: Copyright, Common-Law Alternatives, and Federal Preemption," **63** *N. Car. L. Rev.*, 125-181 (1984), pp. 141-142. Hereafter, this article is cited as "Shipley and Hay."

[17] Rockford Map Publishers, Inc. v. Directory Service Co., 768 F.2d 145, 149 (7th Cir.), reh'g denied, 768 F.2d 145 (7th Cir. 1985).

[18] Shipley and Hay, p. 125 ff.

[19] Shipley and Hay, p. 138 (citations omitted). See also p. 141 ff.

[20] 17 U.S.C. §103 (1982).

[21] Gerritzen, p. 1146, n. 142

[22] Florence v. Department of Defense, 415 F. Supp. 156 (D.D.C. 1976).

[23] A. Van Cook, "Department of Defense Panel," J. Natl. Class. Mgmt. Soc., **12** (No. 2), 29-42 (1977), pp. 39-40.

[24] F.W. May, "Panel - Government Glassification Management Polocies and Programs," *J. Natl. Class. Mgmt. Soc., 2, 76-80 (1966), p. 78.*

[25] G. MacClain, "Special Remarks," J. Natl. Class. Mgmt. Soc., 6, 105-110 (1970), p. 106.

[26] *Information Security Program Regulation, DoD 5200.1-R, U.S. Dept. of Defense, Aug. 1982,* §2-211.

[27] A. L. Thomas, "Application of Security Classification Guides," J. Natl. Class. Mgmt. Soc., **25**, 139-158 (1989), p. 145.

[28] EO 12356, §1.3(b).

[29] A. F. Van Cook, "Information Security and Technology Transfer, An OUSD Overview of Executive Order 12356 and DoD's View Concerning Implementation," *J. Natl. Class. Mgmt. Soc.*, **18**, 1-7 (1982), p. 3.

[30] Taylor v. Department of the Army, 684 F.2d 99, 104 (D.C. Cir., 1982).

[31] Taylor v. Department of The Army, 684 F.2d 99, 104 (D.C. Cir., 1982).

[32] Taylor v. Department of the Army, 684 F.2d 99, 103-104 (D.C. Cir., 1982).

[33] *American Friends Service Committee v. Department of Defense,* 831 F.2d 441 (3rd Cir. 1987).

[34] *American Firends Service Committee v. Department of Defense,* 831 F.2d 441, 445 (3rd Cir. 1987).

[35] *American Friends Service Committee v. Department of Defense,* 831 F,2d 441, 446 (3rd Cir. 1987).

[36] *Handbook of Chemistry and Physics,* 69th Edition, R.C. Weast, ed., CRC Press, Inc., Boca Raton, FL, 1988.

[37] Halperin v. National Security Council, 452 F. Supp. 47 (D.D.C. 1978).

[38] Halperin v. National Security Council, 452 F. Supp. 47, 50 (D.D.C. 1978).

[39] Halperin v. National Security Council, 452 F. Supp. 47, 50 (D.D.C. 1978), affidavit of Z. Brzezinski, Assistant to the President for National Security Affairs.

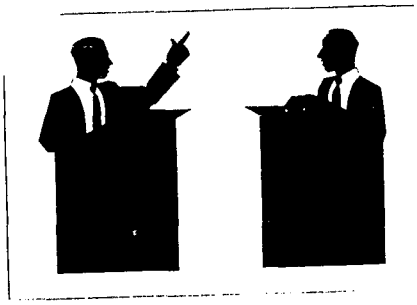
[40] Halperin v. National Security Council, 452 F. Supp. 47, 52 (D.D.C. 1978).

[41] Halperin v. National Security Council, 452 F. Supp. 47, 52, n. 6 (D.D.C. 1978).

[42] Schroeder v. William Morrow & Co., 566 F.2d. 3 (7th Cir. 1977), p. 5.

[43] Rand McNally & Co. v. Fleet Management Systems, Inc., 600 F. Supp. 933 (N.D. Ill. 1984), p. 941.

[44] Shipley and Hay, p. 135, citing Toksvig v. Bruce Publishing Co., 181 F.2d 664 (7th Cir. 1950) and Holdredge v. Knight Publishing Corp., 214 F. Supp. 921 (S.D. Cal. 1963).



THE DECLASSIFICATION DILEMMA:

Are We Heading in the Right Direction?

Robert J. White

Several weeks ago I was enjoying a telecast of our local university basketball game when my number two son interrupted me with the following question:

"Dad, if you are concerned with classified information, how could you permit the existence of classified documents dating back to World War I?"

He was referring, of course, to the ISOO report that World War I troop movement data was still being kept classified Confidential by the Department of the Army.

Well, I did not have anything to do with the situation described by my son, but I was not surprised by the situation he described.

Having been in the industrial security business for many years, I am as aware of the problems resulting from the downgrading and declassification methods adopted by DoD, or lack thereof, as most others in my profession.

Since I am a history nut, I retrieved a copy of the oldest Industrial Security Manual (ISM) that I could find, dated 19 January 1954. To my surprise, I noticed that the terms "declassify" or "declassified" do not appear, only the words "regraded when so advised by the Contracting Officer."

It would appear that the terms "declassification" or "downgrading" were not very common terms in the early days of ISMs.

Since the 1950s, there have been two major downgrading and declassification methods advertised:

- Automatic, Time-Phased
- Originating Agency's Determination Required (OADR)--the present one

I know that this may start an argument when I say that the automatic, time-phased policy was better than the current OADR method. Why? because a "forcing" action occurred, at least part of the time. For example, for the Secret to Confidential levels, the information could be released to more people as it followed the prescribed process: *i.e.*, downgrade to Confidential on _____; declassify on _____. With the OADR you wait, and wait, and wait, and wait.

What are some of the problems created by the lack of a solid downgrading and declassification program?

Space Requirements

Classified material must be stored somewhere and in approved containers. Containers take up space, where unclassified documents can be either:

- Placed in one's desk;
- Taken home for review and safekeeping; or
- Left out entirely in the open.

Costs

If we consider that by July 1998, all classified information will, by necessity, be stored in expen-

sive GSA safes, the problem is magnified. For instance, if a container now stores information in files with a Sargent and Greenleaf padlock, the cost, when compared to the need for a safe, is considerable.

Unnecessary Exposure

Remember the fiasco created when an agency of the government sent some cabinets to the Federal Penitentiary for painting by convicts and failed to check the containers prior to shipping? In all fairness, the classified documents had probably outlived their usefulness and could have been destroyed; or, if a system had been in effect, downgraded and ultimately declassified.

Security Clearance Costs

Since all clearances must now be processed through the Defense Industrial Security Clearance Office, the amount spent on clearances could be reduced with a sound declassification program that works. We thought we had a workable program when industry, government, and other interested parties reviewed the overall system to come up with recommendations in the late 1970s. What did we get? *OADR*! Not exactly the best solution to a major problem. OK. You ask "What should we do?"

Assuming that the new National Industrial Security Program will not address the subject (If so, we can review their ideas!), and that ISOO cannot or will not take over this initiative, the following proposal is submitted:

— Consider of the nature of the data involved: Is there a present, future or alleged threat?

— Is a substitute available that is less volatile?

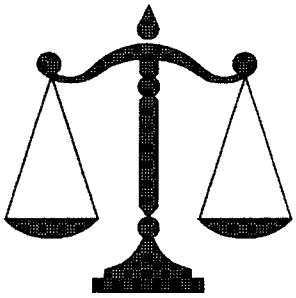
— Who would benefit from the data?

— For what length of time should the data remain classified at its present level?

If there are doubts concerning the time value of the information, I would suggest a 10 year continued classification, then go to the originating agency for an answer. The 20 years is too burdensome on both the contractor and DoD. I know that we can go back to our User Agency for advice on these matters, but the process is slow and deliberate, with the final answer not exactly "just around the corner."

The current philosophy of keeping overhead and floor space costs to a minimum simply will not tolerate a system that insists on maintaining an outdated downgrading and declassification system.

Robert J. White is Director of Security for Cincinnati Electronics Corporation, Cincinnati, Ohio.



DEFENDING CONTRACTOR EMPLOYEES IN SECURITY CLEARANCE REVOCATION PROCEEDINGS:

A Guide for Defense Counsel

Jack Thomas Tomarchio

This paper discusses the defense of Government contractors at security clearance revocation hearings. It is meant to be a practical guide for defense counsel involved with Government contracts and industrial security. As such, it suggests tactics and techniques that can be utilized in defending Government contractor employees facing security clearance suspension or revocation procedures. This is not an exhaustive study of the state of personnel security clearance law, nor does it deal with the discussions in Congress regarding changes to DoD Directive 5220.6, subject: "Industrial Personnel Security Clearance Program." Such matters are beyond its scope.

The issues in this article are presented through case study. Specific reference is made to an actual case tried before the Directorate for Industrial Security Clearance Review (DISCR), an administrative judge, and the DISCR Appeal Board (appeal board). To safeguard client confidentiality, the names and facts have been significantly altered.

FACTUAL SCENARIO

Applicant was the president and sole stockholder of a small business located in south central New Jersey. The applicant's company manufactured sophisticated guidance and communication circuitry for satellites and military telecommunication devices. Approximately 85% of its work involved classified Government contracts for which a Secret clearance was required. A bulk of the company's work was employed in the Strategic Defense Initiative or "Star Wars" program. The applicant had been granted a Secret personnel security clearance while his company (Rambo, Inc.) was granted a Secret facility clearance.

On February 9, 1991, the applicant was notified by DISCR that a review of his eligibility for a security clearance had been made pursuant to Executive Order 10865, as amended, and as implemented by DoD Directive 5220.6. As a result of this review, DISCR was unable to find that it was clearly consistent with the national interest to grant the applicant access to any classified information, and recommended that the applicant's case be submitted to an administrative judge for determination whether to deny, suspend, or revoke the applicant's security clearance.

The reasons for this action were spelled out in a Statement of Reasons (SOR) and included the following allegations:

> *Criterion G:* Available information reflects disregard of public law, statutes, Executive Orders or regulations including violations of security regulations or practices on your part. That information is:
>
> a. You authorized and/or directed your executive secretary to be issued government travel orders, representing her as a qualified GS-12 (equivalent) engineer with a Secret clearance, so that she could travel to the Republic of Korea to perform on a U.S. Air Force contract during August 1987, in violation of paragraphs 3.e, 20.a, 20.b., 24.a., 26.a. and 26.b., of the Industrial Security Manual for Safeguarding Classified Information and Title 18, United States Code, Section 798.a.
>
> b. You authorized the issuance of a Company Confidential clearance to your executive secretary on August 10, 1987, the date of

your secretary's departure for the Republic of Korea to perform on the U.S. Air Force contract. This authorization is in violation of paragraphs 20.c. (1) and 14.b. of the Industrial Security Manual for Safeguarding Classified Information.

Criterion H: Available information tends to show dishonest conduct on your part. That information is:

a. That information set forth under paragraph 1., above.

b. In a signed, sworn statement dated October 5, 1988, and presented to a Special Agent of the Defense Investigative Service, you falsified or misrepresented material facts in that you stated you had done undergraduate work in Nuclear Engineering and graduate work in Mathematics at the University of Arizona, where in truth and in fact, as you then and there well knew and sought to conceal, you had done neither of these things.

c. In response to a North Carolina Transit Corporation (NCTC) Pre-Qualification Application, executed by you on/about December 16, 1986, you represented RAMBO, Inc., as a minority-owned business, which claim you then knew to be false.

d. You executed a North Carolina Transit Corporation Minority Business Form C on December 21, 1986, in which you declared and affirmed under oath that RAMBO, Inc., was a minority-owned business, which declaration and affirmation you then knew to be false.

e. You executed a North Carolina Transit Corporation Minority Business Form C on December 7, 1986, in which you declared and affirmed under oath that RAMBO, Inc., was a minority-owned business, which declaration and affirmation you then knew to be false.

f. You surreptitiously recorded a telephone conversation which took place on/about August 10, 1987, between yourself, George Hones and Rick Dixon, without the knowledge or consent of either of the other two persons involved, and then directed that this tape recording be transcribed into a typed document, in violation of Federal Law.

Criterion I: Information set forth under paragraphs 1. and 2., above, tends to reflect acts of omission or commission that indicate poor judgment, unreliability or untrustworthiness on your part. [The criteria cited above will be found in Section F.5. of the referenced DoD Directive 5220.6.]

Following review of the SOR and an interview with the applicant, defense counsel filed an answer with DISCR on February 23, 1991, specifically denying each and every allegation in the SOR.

This process was established over the past 45 years as part of the Defense Industrial Security Program. A brief background will illustrate our current state of procedures developed.

DEVELOPMENT OF THE INDUSTRIAL SECURITY PROGRAM

The Defense Industrial Security Program arose out of World War II when Government contractors were required to perform classified work in defense contracts:

At the outset, each Armed Service Branch administered its own industrial clearance program. In 1947, the Department of Defense and the Secretaries of the Armed Services established a centralized program headed by the Army-Navy-Air Force Personnel Security Board (PSB) and the Industrial Employment Review Board (IERB) that implemented generalized procedures for security clearances. Authority for instituting such a program was derived through implication from the National Security Act of 1947. The PSB and the IERB were replaced by the Industrial Personnel Security Board (IPSB) in 1953 that promulgated the Industrial Personnel Security Review Regulation.[1]

In combining these boards, the Secretary of Defense provided that:

The Army, Navy and Air Force shall establish such number of geographical regions within the United States as it seems appropriate to the workload in each region....[Each region was to establish] an Industrial Personnel Security Board, [,to]...consist of two separate and distinctive divisions, a Screening Division and an Appeal Division, with equal representation of the Departments of the Army, Navy and Air Force on each such division. The Appeal Division was given jurisdiction to hear ap-

peals from the decisions of the Screening Division.[2]

The first challenge to the Industrial Security Regulations came in 1959 when the U.S. Supreme Court decided *Greene v. McElroy*.[3] In *Greene*, a civilian aeronautical engineer was deprived of his security clearance because he had been found to have associated with members of the Communist Party and military officers attached to the Russian Embassy in Washington, D.C. The petitioner appealed, arguing in hearings before the Industrial Employment Review Board and the Eastern Industrial Personnel Security Board that he "had no opportunity to confront and question persons whose statements reflected adversely on him or to confront Government investigators who took their statements."[4] The Court agreed with the petitioner, holding that in the absence of explicit authorization from the President or Congress, the respondents were not empowered to deprive the petitioner of his job in a proceeding in which he was not afforded the safeguards of confrontation and cross-examination.[5] Accordingly, the Court reversed the decisions of the boards which had stripped the petitioner of his security clearance.

In response to the Supreme Court's criticism of the Industrial Security Program then in place, President Eisenhower issued Executive Order 10865[6] entitled "Safeguarding Classified Information Within Industry." This Order prohibited the final denial or revocation of a security clearance until an individual had been afforded the following procedural safeguards: (1) A written statement of the reasons why access to classified information may be denied; (2) opportunity to reply in writing; (3) opportunity for a hearing after the filing of a written reply to the Statement of Reasons; (4) reasonable time to prepare for the hearing; (5) opportunity to be represented by counsel; (6) opportunity to cross-exam persons on matters not relating to the characterization of any organization or individual other than the applicant; and (7) written notice of the final decision concerning the allegations contained in the Statement of Reasons.[7]

The Department of Defense promulgated DoD Directive 5220.6 on December 7, 1966 which delegated to the Assistant Secretary of Defense (Administration) [ASD(A)] the responsibility for the control of access by individual personnel to classified information and provided for the delegation by the ASD(A) of a screening board to consider initially all cases involving the denial or revocation of an industrial security clearance.[8] The directive also authorizes the screening board to investigate any individual whose clearance is being investigated; entitles the applicant to be issued a formal SOR outlining the reasons for possible suspension or revocation of his clearance; entitles the applicant to a formal hearing if he requests one; entitles the applicant to the full panoply of procedural due process that the executive order envisioned; and provides the applicant with the right to appeal adverse decisions to an appeal board.[9]

DoD Directive 5220.6 charges the Defense Industrial Security Clearance Office (DISCO) with making the preliminary determination whether it is clearly consistent with the national interest to grant or continue a security clearance for access to classified information by persons employed by U.S. industry.[10] Once a determination is made that it is not consistent with the national interest to grant such a clearance, the case must be referred from DISCO to DISCR.[11]

Upon referral, DISCR then makes the determination promptly whether to grant or continue clearance, to issue a Statement of Reasons as to why it is not clearly consistent with national interest to do so, or to take whatever interim actions it determines are necessary. Such actions include (a) conducting further investigation, (b) propounding written interrogatories to the applicant or other persons with relevant information, (c) requiring the applicant to undergo a medical evaluation by a DoD psychiatric consultant, or (d) interviewing the applicant in order to reach a final determination.[12]

Upon receipt of the SOR, the applicant has 20 days to submit his answer to DISCR. The answer must be under oath and must admit or deny each and every allegation in the SOR. A general denial is not sufficient.[13] It is usually at this stage in the proceedings that counsel is called in to provide representation to the applicant. Counsel's work at the early stages of the proceedings is critical, as many cases can be won or lost prior to litigation commencing.

PRE-TRIAL REPRESENTATION: TACTICS AND STRATEGIES

a. Initial Representation

Faced with litigating against the Government, counsel will often feel that the cards are

stacked against them. This feeling is enhanced in security clearance cases, which carry the heightened sense of urgency that pervades national security matters. Presented with Government prosecutors and investigative agents who are inflexible in their resolve and supported by the seemingly unlimited power of the United States, many counsel feel helpless. Nevertheless, these situations are often not as bleak as they may seem and applicants, if provided with aggressive and creative counsel, can often increase their chances of success later at the hearing.

Aggressive representation would start as soon as the applicant is put on notice that he is the subject of security clearance revocation proceedings. Often, as in this study case, that occurs when the applicant receives a copy of the SOR from DISCR. Upon receipt of the SOR, counsel needs to interview the applicant immediately, since the SOR must be answered within 20 days of receipt.[14] During the initial review, counsel should go over each allegation with the applicant to ascertain its truth or falsity and to discuss possible defenses. Counsel and the applicant also need to determine whether the applicant will seek a hearing or simply submit documents to refute the allegations contained in the SOR.

At the early stages in the proceedings, counsel should explore alternative means of case disposition. Often cases referred to DISCO can be disposed of through coordination with Government officials. Some cases being investigated by DISCO are the result of misunderstandings or lack of information. Defense counsel, faced with such situations, should contact the personnel security representative at DISCO and attempt to set up a meeting with Government representatives and the applicant to discuss the case and seek ways of resolving the controversy short of litigation.

When the case has reached DISCR level, the defense options to dispose of the case in the pretrial stages diminish significantly. While inquiries should still be made to Government counsel regarding settlement of the case, such inquiries usually are not well received. Attempts to exercise a political option on behalf of an applicant by enlisting the aid of elected officials have uniformly proven unsuccessful and should be avoided.

b. Discovery

Discovery in DISCR cases is limited. DoD Directive 5200.6 states that "discovery by the Applicant is limited to documentary material in DISCR files."[15] Defense counsel should make maximum use of available discovery tools by filing a Request for Discovery with DISCR counsel, and at the same time a Freedom of Information Act (FOIA) request with DISCR. These parallel discovery avenues will often prove fruitful with each request providing documents not obtained from the other request.

In the study case, documents received pursuant to the FOIA request proved to be more illuminating than the documents received from DISCR counsel in response to the Request for Discovery. Since DoD Directive 5220.6 does not allow for any other forms of discovery (*e.g.*, depositions, interrogatories, and requests for admissions), such tools are usually not available to counsel in preparing the defense of a security clearance revocation proceeding. Nevertheless, discovery of the Government's case can often be accomplished through the use of collateral proceedings.

In the study case, the applicant was being investigated for actions he took while he was an employee of Rambo, Inc. Prior to the DISCR investigation, the applicant was terminated from Rambo by a vote of the company's board of directors. The termination of the applicant was followed by a report submitted to DISCR that his actions, while an employee of Rambo, were inimical to the best interests of national security. This report was authored by the president of Rambo and submitted on behalf of the board of directors. Utilizing this letter, which the applicant contended contained false and misleading information regarding the nature of his activities, the applicant filed suit in state court alleging defamation and wrongful discharge. This suit was filed two weeks after the applicant's receipt of the SOR. Using this collateral lawsuit, defense counsel was able to submit interrogatories and requests for production of documents to the defendants in the state court action, many of whom were expected to be Government witnesses at the security clearance hearing.

The applicant's counsel may also wish to take depositions of the witnesses in the pending collateral state case who he anticipates will testify for the Government at the security clearance hearing. In addition to obtaining "free discovery" on the security clearance case, defense counsel can also lock potential adverse witnesses into their testimony at the deposition. Should the same witnesses testify at the security clearance hearing, they will be bound by their testimony given at the deposition.

The filing of a collateral lawsuit can also be used to bar certain witnesses from testifying at the security clearance hearing. Under present DISCR regulations, the Government does not enjoy the power to subpoena witnesses for security clearance hearings.[16] In the study case, the collateral state lawsuit file against the applicant's former employer was effectively used to bar the testimony of four potential witnesses who were defendants in the state court action. These witnesses were faced with the prospect of voluntarily testifying at the security clearance hearing and thereby possibly endangering their cases at the state court level. The witnesses, on advice of their counsel, chose not to testify at the security clearance hearing so as not to harm their cases in the state court action. Since DISCR counsel lacked subpoena power, he could not compel these individuals to offer testimony at the hearing.

While it is recognized that collateral lawsuits may not be appropriate in every case, defense counsel should examine the possibility of a collateral lawsuit being filed as both an offensive (discovery) weapon, and as a defensive tactic to deprive DISCR counsel of potential witnesses in the security clearance revocation hearing.

c. Staying Proceedings

Many of the charges which give rise to security clearance revocation hearings also involve allegations of criminal misconduct. As such, these charges may serve as the basis for criminal proceedings in State and Federal Courts, or as charges in debarment or suspension actions. In the study case, the applicant was charged with violations of the United States Code and with allegations which could constitute fraud against the United States Government. Defense counsel should be aware of the possibility that an applicant may face criminal charges or a suspension or debarment proceeding based on the same set of facts involved in the security clearance hearing. Defense counsel cognizant of this possibility should consider seeking a stay of the security clearance proceeding until the criminal charges are disposed.

Given that a security clearance hearing would most likely take place before any indictment was handed down, there exists a distinct possibility that evidence given by the applicant during a security clearance hearing may be used against the applicant in obtaining a criminal conviction. Concurrently, testimonial evidence by an applicant may constitute a waiver of the applicant's Fifth Amendment right not to testify against himself. Accordingly, defense counsel should ensure that any prior or pending hearings, occurring before the criminal procedures are complete, be stayed.

In *E-Systems, Inc.*,[17] the board denied the Government's request for a stay of the board's hearing pending the resolution of concurrent criminal proceedings.[18] In that case, a board hearing was about to be held regarding the contractor's alleged wrongful termination, the Government's improper changing of contract standards, and compliance of the contractor's quality assurance system with Government requirements. Although no criminal action was actually pending, there was an ongoing joint Criminal Investigative Division-Federal Bureau of Investigation examination regarding the contractor's alleged falsification of test data. The board held that the Government had failed to show there was an overall need to protect the criminal action; that any prejudice would result to the Government if the board hearing was not stayed; and that there was insufficient similarity between the issues, facts and witnesses in the two proceedings. However, the board did postpone the actual hearing itself pending resolution of the criminal matter because it decided that evidence developed by the Government during its investigation might be a defense to the contractor's evidence regarding his right to damages. Thus although an outright stay was denied, the actual hearing was put off apparently to permit the Government an opportunity to present its best evidence at the hearing.

In *Tyger Construction Company,* [19] the Government's request for a stay of a board hearing was denied because the concurrent criminal action was only in the investigatory stage. Citing the decision in *E-Systems*, the board distinguished *Tyger* by concluding there was no showing that any evidence to be developed in the Government criminal investigation would affect the board's ability to determine the facts of the current appeal.[20]

In *Afro-Lecon, Inc. v. U.S.*[21], the court considered a request by a contractor to stay a civil proceeding during the pendency of a parallel criminal action brought against the contractor. The court held that the mere fact the applicant was responsible for bringing the appeal in the first place did not automatically deprive him of the right to assert a Fifth Amendment privilege against giving testimony in the civil appeal during the pendency of the criminal action, stating that "procedure should not require a party to surrender one's constitutional

testimony in the civil appeal during the pendency of the criminal action, stating that "procedure should not require a party to surrender one's constitutional right in order to assert another." [22] The court also noted that, because appellant requested merely a stay of the civil proceedings, the contractor did not raise the problem of putting the defendant in the position of maintaining a defense without being able to obtain discover.[23] Accordingly, the court held that the board should re-examine the case and determine whether the interest of the appellant in staying the proceedings was outweighed by the interest of the Government in prosecution of the claim before the Board.[24]

In the case of *Skip Kirchdorfer, Inc.*[25], the board considered a request by a contractor that the board appeal be stayed pending a criminal investigation by the Government. Initially, the board, while acknowledging the contractor's Fifth Amendment right, held that a stay would not be granted because there were, in fact, no parallel proceedings meriting the granting of a stay. The board found that the appellant had failed to show that there was substantial similarity in the issues, facts and witnesses in the two proceedings. To the contrary, the board found the ongoing grand jury investigation concerned only one contract and there was no indication that it was the same contract as that being considered in the board appeal. As a result, the board found it unlikely that the countractor would be forced to choose between foregoing his constitutional rights or the corporation's rights to recover money allegedly due it by the United States.

In a later proceeding,[26] the contractor presented evidence that the Defense Criminal Investigative Service and the Air Force Office of Special Investigation had served subpoenas on two of the appellants' senior officers. Representatives of those agencies had stated that they were engaged in conducting an investigation of those officers for the purpose of criminal prosecution. In light of this new evidence, the board stated "it is abundantly clear that a criminal investigation is in fact in process," and "the matter of staying the appeals pending the results of the criminal investigation is a matter that needs fuller briefing and evidentiary submittals by the parties."

Finally, in yet a later proceeding,[27] the board held it had been revealed that the only ongoing criminal investigation involving the contractor concerned another contract during an earlier time at another Air Force base. Additionally, the subpoenas has been served only to obtain depositions in the appeal pending before the board. As a result, the board found no nexus between the ongoing criminal investigation and the instant appeal, and therefore denied the contractor's request for a stay of proceedings.[28]

As the foregoing cases have made clear, *a stay of the civil proceedings is generally not favored.* That is, absent a showing of concurrent criminal and civil actions and similarities of issues and facts in the two cases and prejudice to the moving parties, a stay of the civil or administrative proceedings usually will not be granted. On the facts of the study case, it was anticipated that the issues in any possible criminal proceeding would probably have been exactly the same issues as those in the security clearance revocation hearing. That is, the issues to be decided in both fora would be the net effect of the applicant's alleged misuse of security clearance procedures. The facts underlying the allegations would also most likely have been the same in both proceedings: the wrongful granting of security clearances, the violation of the United States Code with regard to wire tapping, and various allegations of Government contract fraud. Prejudice incurred from a stay of the security clearance proceedings would probably have been outweighed by the prejudice which might result from continuing a security clearance hearing, in light of a pending criminal indictment.

In the study case, counsel was prepared to argue that if the security clearance revocation proceeding was not stayed, the applicant would be put in the unenviable position of having to choose between foregoing his Fifth Amendment right to self-incrimination or foregoing his right to defend himself at the security clearance hearing. Counsel was prepared to argue that the Government would probably be put at a disadvantage to the extent that it was unable to engage in meaningful discovery because of the applicant's assertion of his Fifth Amendment right not to give testimony which might be self-incriminating. In the study case, had an indictment been issued prior to the security clearance revocation hearing, counsel was prepared to argue that judicial resources would not be put to their most efficient use if the security clearance hearing could make little or no headway because of the applicant's assertion of the Fifth Amendment privilege.

On the other hand, defense counsel should be aware that, when criminal proceedings are in a

investigatory stage, the hearing body may consider the stay of proceedings premature. That is, because an applicant would, of necessity, only be able to speculate that the Government would eventually hand in an indictment (or even start grand jury proceedings), the hearing body may not be sufficiently satisfied that there are ongoing proceedings of a criminal nature sufficient to justify staying a security clearance hearing. Nevertheless, defense counsel should be prepared to argue the reasoning posited in the *Skip Kirchdorfer*[29] case, which indicated at least a willingness to consider a request for a stay while a criminal investigation was ongoing. Accordingly, it appears that those cases where an indictment has been handed down will be the ones in which the defense will be most successful in obtaining a stay of the security clearance hearing until the criminal indictment proceedings have been concluded.

In the study case, the Government opted not to indict the applicant criminally, thus obviating the need to apply for a stay of the security clearance proceedings. Defense counsel faced with a situation wherein a criminal indictment is anticipated, and indeed, expected, should seriously consider the stay option, and should consult the line of cases cited.

d. Suspension and Debarment

Security clearance proceedings may be the first step in a process which leads to the eventual suspension or debarment to contract with the United State Government. In these scenarios, defense counsel will want to research what affect the security clearance hearing will have upon subsequent suspension or debarment proceedings. A primary question in this regard concerns whether issues of fact decided in a security clearance hearing would be collateral estoppel (restraint) as to later suspension and debarment proceedings.

It is generally recognized that an administrative hearing that contains the procedural protections afforded by judicial hearings may collaterally estop (preclude) later administrative or civil proceedings based upon the same issues of fact:

> An adjudicative determination by an administrative tribunal is conclusive under the rules of *res judicata* (unalterable precedent) only insofar as the proceedings resulting in the determination entailed the essential elements of adjudication, including:
>
> (a) Adequate notice to persons who are to be bound by the adjudication, as stated in § 2;
>
> (b) The right on behalf of a party to present evidence and legal argument in support of the party's contentions and fair opportunity to rebut evidence and argument by opposing parties;
>
> (c) A formulation of issues of law and fact in terms of the application of fact in terms of the application of rules with respect to specified parties concerning a specific transaction, situation, or status, or a specific series thereof;
>
> (d) A rule of finality, specifying a point in the proceeding when presentations are terminated and a final decision is rendered; and
>
> (e) Such other procedural elements as may be necessary to constitute the proceeding a sufficient means of conclusively determining the magnitude and complexity of the matter in question, the urgency with which the matter must be resolved, and the opportunity of the party to obtain evidence and formulate legal contentions.[30]

In *Ramone-Sepulveda v. INS*,[31] the court held that the Immigration and Naturalization Service (INS) could not institute the deportation hearing for a second time based upon the same facts adjudicated in a previous administrative hearing. In that case, the administrative judge in the previous hearing had held that the INS had failed to prove that the defendant was an alien. INS tried to reinstitute the deportation proceedings on the basis that it was proceeding upon newly discovered evidence. The court held that the allegedly new evidence was not, in fact, only recently discovered and, therefore, the INS was estopped by the prior proceedings.

Similarly, in *Pantex Tilling Corp. v. Glidewell*,[32] the court held that issues of fact previously decided by the National Labor Relations Board (NLRB) estopped a later tort action by the plaintiff. In that case, the NLRB had decided that the plaintiff Pantex had failed to prove that a work stoppage by the defendants created an existence of potential risk of substantial property damage to the plaintiff's property. The plaintiff attempted to institute a civil proceeding in tort based upon the alleged existence of unsafe conditions posing a risk to his property. The court held that the plaintiff was

estopped from instituting that proceeding based upon the collateral estoppel effect of the prior administrative hearing.[33]

Under Federal Acquisition Regulations,[34] a suspending official may suspend a contractor based upon numerous, broadly defined acts or omissions. The suspending official may suspend a contractor suspected, upon adequate evidence, that the individual was engaged in the commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public contract or subcontract. The suspending official may, upon adequate evidence, also suspend a contractor for an action of so serious or compelling a nature that it affects the responsibility or a Government contractor or subcontractor to perform successfully a current contract.

Given the plenary authority in the hands of the suspending official, it appears unlikely that previous administrative hearings or decisions will have any power to delay or stay proceedings by the suspending official. Essentially, the fact issues decided in the previous administrative hearing may simply be irrelevant to the suspending official's determination. This is so because, even if the previous administrative hearing determines that the contractor did not engage in acts sufficient to constitute fraud, such a decision will be insufficient to foreclose the possibility that the actions were "so serious or compelling "as to affect "present responsibility of a Government contractor or subcontractor." That is, the fact issues decided in the previous administrative hearing may only be preclusive in regards to the suspension or debarment hearing *to the extent* that the previous administrative hearing finds *that the underlying facts* (*e.g.*, the acts mentioned in the SOR) *were not proven at all.* Otherwise, even if the previous administrative hearing determines that the contractors did not engage in "improper conduct" sufficient to make him liable for some remedy, the suspending official would probably still be permitted to make the factually distinct decision as to whether the conduct of the contractor affects his present responsibility.

Further, even if the result of a security clearance hearing is that the available information does not reflect "disregard of public law, statutes, Executive Orders or regulations, including violations of security regulations," such a finding may be insufficient to preclude the suspending officer from finding that the acts complained of affect the responsibility of an applicant as a Government contractor. Not only does it appear that there are two distinct factual inquiries, the difference may also be construed as distinct "policy considerations" that outweigh the judicial economy concerns underlying the doctrine of collateral estoppel.[35] Accordingly, it does not appear that a suspending official or debarring official will be collaterally estopped from debarring or suspending an applicant based upon the same facts presented at the security clearance hearing.

TRYING THE CASE

Security clearance cases run from simple allegations of wrongdoing, usually involving a relatively uncomplicated set of facts, to complex cases often involving numerous witnesses and documentary evidence. In either simple or complex cases, the role of the defense counsel remains the same, to prove that it is clearly consistent with the national interest to grant or continue a security clearance for the applicant.[36] Unlike criminal cases, defense counsel cannot simply rely upon the department counsel's inability to prove his case against the applicant. Rather, the DoD Directive puts the burden on both counsel to prove that either the applicant should not retain his security clearance or, conversely, that the applicant should be permitted to retain his clearance.

Since DoD Directive 5220.6 does not permit motion practice, pre-trial motions, motions *in limine* (*i.e.*, request made before trial or having to request protection against prejudicial questions and statements), motions to dismiss, and motions for specific findings are not available; therefore, counsel should be prepared to try his case "to verdict."

Complex security clearance cases are, more often than not, document intensive. As such, defense counsel should prepare a workable document retrieval system. The study case involved over 3,000 documents and over 80 exhibits with some exhibits containing 50 to 100 pages. A trial notebook and binders containing both Government and defense exhibits should be prepared and brought to the trial for easy reference.

Defense counsel's thorough preparation should lead him to develop his theory of the case at an early stage. In the study case, the defense theory revolved around a business dispute between the applicant and board of directors of his former corporation, Rambo, Inc. In support of this theory, defense counsel introduced numerous memoranda

and correspondence reflecting the gradual deterioration of the relationship between the applicant and his board of directors which eventually led to the applicant's termination.

The defense theory of the case should be established early on at trial, and should be presented forcefully during opening argument. After opening argument, the defense counsel should continually seek every opportunity to present the defense theory of the case to the administrative judge. This can be done effectively through cross-examination of the Government's witnesses. Of course, in the study case, the defense had been successful in depriving the Government of several witnesses by filing a collateral lawsuit in state court.

Most often, the Government's case will consist of the applicant' chief accusers, co-workers and Government investigators. The Defense Investigative Service (DIS) is the Governmental authority charged with investigating security clearance matters. DIS investigators will often testify at the hearing regarding the results of their investigation; these investigators are subject to cross-examination. In the study case, great success was achieved in cross-examining DIS investigators to reveal the flaws in their investigation. Specifically, it was shown that the DIS investigators failed to obtain a complete copy of the Government contract referred to in paragraph 1(a) of the SOR; failed to interview the contracting officer who administered the same Government contract; failed to determine whether the applicant had received transfer credits in electrical engineering from another university; failed to check the definition of "minority-owned business" in North Carolina Transportation Corporation regulations; and failed to interview parties to an alleged illegally tapped conversation to ascertain whether they had consented to the taping of that discussion.

Further headway can also be made in the cross-examination of the applicant's co-workers. By establishing the fact that a business dispute existed between the applicant and his co-workers, defense counsel in the study case was able to explore such issues as motive and bias when probing these witnesses.

Documentary exhibits are often used by both sides during the course of the trial. Although the rules of evidence are not slavishly followed, they are used as a guide.[37] In practice, this allows the administrative judge to receive just about anything into evidence while assigning each exhibit the weight that he thinks it merits. Nevertheless, defense counsel should aggressively oppose introduction of evidence that does not comport with the traditional rules of evidence. In the study case, defense counsel raised objections on relevancy, hearsay, ultimate issue, unqualified expert testimony and prejudice grounds. Several of the objections were sustained by the administrative judge, while others were admitted but with restrictions. Since the revocation proceeding is appealable to the DISCR Appeal Board, defense counsel should raise evidentiary objections and "build a record" for appellate purposes.

During the defense case in chief, consideration should be given to presenting the testimony of the applicant to rebut the charges against him. Of course, this decision should be carefully weighed against the potential harm that could inure to the applicant should he take the stand and subject himself to cross-examination.

Defense counsel should also seek testimony of witnesses who will refute each allegation contained in the SOR. Such testimony should be directed only to the charges pending against the applicant and not be burdened by references to the applicant's good record. Separate testimony may be offered, after the merits, regarding the applicant's good character in the community. Reputation testimony can be offered through live witnesses or through the introduction of a Stipulation of Expected Testimony.

Defense counsel should aggressively seek to obtain as many character witnesses (either in person or via stipulation) as is practical, and should attempt to draw these witnesses from the applicant's business and social contacts.[38]

After closing the defense case in chief, the administrative judge often allows rebuttal by the department counsel and surrebuttal by the applicant's counsel. Following rebuttal, both sides can present closing arguments, with the department counsel retaining the right to a short rebuttal of the applicant's argument.

Closing argument is the applicant's counsel's last opportunity to drive home the defense theory of the case and should be used for this purpose. Upon the close of the record, a transcript shall be made of the hearing, with the applicant and department counsel being furnished one copy of the

transcript plus the exhibits without cost.[39] The administrative judge is directed to provide written finding of fact with respect to each allegation contained in the SOR within 30 days following the close of the hearing record. Normally, administrative judges take longer than the 30 days mentioned in DoD Directive 5220.6[40].

POST HEARING PROCEDURES AND REPRESENTATION

Upon receipt of the administrative judge's decision, the applicant or department counsel may appeal the determination by filing a written Notice of Appeal within 20 days after the date of the determination. The appeal must be in writing and must be filed within six days after the date of the administrative judge's determination. A written reply may be filed by the other party in the case within 30 days of receipt of the copy of the written appeal.[41]

Paragraph 19 of Enclosure 1 of DoD Directive 5220.6 discusses the format in which an appeal must be made:

> *The written appeal must state the specific issues raised on appeal, must cite relevant portions of the case records supporting the issues, and must state the reasons why the determination should be reversed. Consideration of an appeal shall be limited to information in the case record and the issues raised in the written appeal and written reply. The Appeal Board may take action with respect to matters of law raised by the parties to ensure that the Hearing Examiner's ruling(s) were not arbitrary or capricious. Factual findings shall not be disturbed on appeal if such findings are supported by credible evidence and are not contrary to law. No new testimony or evidence shall be considered.*[42]

The appeal board made up three DISCR administrative judges may affirm the determination of the administrative judge or may return it to the administration judge with instructions for further action.[43] The appeal board's decision is final, except in cases where evidence was received that could not be inspected by the applicant because it was classified, or was a written or oral statement by an adverse witness whom the defendant was not able to cross-examine.[44]

The study case witnessed a complete vindication of the applicant, with the administrative judge deciding each and every allegation in the SOR in the applicant's favor. In cases where the applicant is granted a security clearance or retains his clearance, the applicant may apply for attorney's fees.

While DoD Directive 5220.6 does provide for reimbursement for counsel's fees, the provisions of the directive only allow an applicant to petition for reimbursement in cases "resulting directly from a suspension, revocation, or denial of clearance." In cases where an applicant never had his clearance suspended, denied, or revoked, but rather held his clearance throughout the full adversarial hearing, the directive is silent on the subject of reimbursement. Defense counsel faced with this situation where reimbursement is not authorized by the directive should look at other alternatives for recovery of counsel's fees. DISCR contends that legal fees and costs may not be recovered through the use of the Equal Access to Justice Act (EAJA).[45] DISCR grounds its reasoning on the decision of the Seventh Circuit Court of Appeals in *Smedberg Machine and Tool Incorporated v. Donovan.*[46] The court in *Smedberg* held that EAJA did not provide for attorney fees awards to employers who prevailed in proceedings to obtain labor certifications from the United States, reasoning that "unless an agency hearing is statutorily mandated, the EAJA does not provide for the award of attorney fees to the prevailing party."[47] Since, as DISCR reasons, an applicant can elect a hearing before an administrative judge if he chooses, the agency hearing is not "statutorily mandated" such that EAJA would apply.

Since the DoD Directive 5220.6 *only* provides for reimbursement of legal fees in those cases resulting directly from the suspension, revocation, or denial of a clearance, applicants who retained their clearances throughout the DISCR adjudicatory process are deprived of a vehicle to recover legal fees and lost earnings. Possibly an equal protection challenge could be advanced to challenge this statute.

CONCLUSION

As is apparent from this case study, the defense of the contractor in a security clearance revocation proceeding can be a complex, daunting,

and frustrating procedure. Nevertheless, creative lawyering, aggressive tactics, and a good understanding of the interrelationship between collateral proceedings can provide the defense counsel with several weapons to conduct a successful defense. It is hoped that this article will provide security professionals with an appreciation of the tactics, strategies, and methods employed when defending contractor employees facing revocation of their security clearances.

Jack Thomas Tomarchio practices law with the Philadelphia and Washington, D.C. firm of Saul, Ewing, Remick and Saul where he specializes in Government contracts, construction litigations, and international business.

FOOTNOTES

[1]Barton and Peterson, *Industrial Security Clearances: Heightened Importance in a World of Corporate Acquisitions, Takeovers, and Foreign Investments,* 18 Public Contract Law Journal 394 (1989).

[2]20 Fed. Reg. 1553.

[3]360 U.S. 474 (1959).

[4]*Id.*, at 479.

[5]*Id.*, at 508.

[6]25 Fed. Reg. 1583, *as amended,* 3 C.F.R. 512 (1968).

[7]*Clifford v. Shoultz*, 413 F.2d 868, at 870 (1969).

[8]*Id.*, at 871.

[9]DoD Directive 5220.6, August 12, 1985.

[10]*Id.*, para. (B) (3).

[11]DoD Directive 5220.6 (Encl. 1), para, 1 August 12, 1985.

[12]*Id.*, para. 2.

[13]*Id.*, para. 4.

[14]Counsel may apply to the Director of DISCR for a reasonable extension of time. See DoD Directive 5220.6 (encl. 1), para. 4, May 12, 1985.

[15]DoD Directive 5220.6 (Encl. 1) para. 8, May 12, 1985.

[16]DISCR has recently proposed a revision to its regulations which will empower DISCR counsel to subpoena witnesses for security clearance revocation proceedings.

[17]ASBCA No. 32033, *et al.* 88-2 BCA, ¶ 20753.

[18]The vast majority of cases deciding requests for a stay of proceedings involved a request for a stay brought by the Government. This is so apparently because the Government usually wishes to have the board hearing stayed so that the contractor may not use civil discovery to probe the Government's criminal investigative files.

[19]ASBCA No. 34235, 88-3 BCA ¶ 21,148.

[20]See also *Atlantic Garages, Inc.*, GSBCA No. 5891, 81-1 BCA ¶ 15, 132 (Government request for a stay during criminal investigation denied by discovery in appeal limited to protect criminal action); *Ingalls Ship Building Division, Lytton Systems*, ASBCA No. 22645, 78-2 BCA ¶ 13,350. (Contractor's need for a resolution of the board appeal was compelling and was not offset by the Government's need to protect the ongoing criminal proceedings).

[21]820 F.2nd 1198 (Fed. Cir. 1987).

[22]*Id.*, at 1205.

[23]*Id.*

[24]*Id.*, at 1206.

[25]ASBCA No. 82-637, 88-3 BCA ¶ 20,985.

[26]88-3 BCA ¶ 20,985.

[27]89-1 BCA ¶ 21,340.

[28]*See also Ingalls Ship Building, supra,* (where discovery in the appeal may impinge upon the criminal matter pending, a protective order may sufficiently protect the parties' rights); *Jackson Lumber Co.*, ASBCA No. 80-160-1, 81-1 BCA, ¶ 14, 998 (given that the contractor in the ongoing board appeal could have asserted its Fifth Amendment right to not give testimony, the Government's right to discovery would be severely limited; a stay of the Board proceedings was therefore justified); *U.S. v. Kordel.* 397 U.S. 1 (1970) (appellant should assert his Fifth Amendment right during the civil proceedings so as to prevent the use of self-incriminating testimony in later criminal proceedings); *SEC v. Dresser Industries, Inc.*, 628 F.2d 1368 (D.C. Cir. 1980) (appellant's assertion of the Fifth Amendment

privilege may suggest a need for a protective order limiting the scope of discovery).

[29]ASBCA No. 82-637, 88-3 BCA ¶ 20,985.

[30]RESTATEMENT (Second) *Judgements*, § 83.

[31]824 F.2d 749 (9th Cir. 1987).

[32]763 F.2d 1241 (11th Cir. 1985)

[33]*Id.* at 1247. *See also Facchiano v. U.S. Department of Labor*, 859 F.2d 1163 (3d Cir. 1988) (HUD debarment was sufficiently adjudicatory and final to enable appellants to raise a preclusion defense in later DOL debarment proceedings); *U.S. v. Temple*, 299 F.2d 30 (7th Cir. 1962) (United States' pursuit of a single cause of action which had alternative remedies led to a merger of the cause of action in the judgment and prevented maintenance of a second action to pursue the alternative remedy); *Connecticut Light and Power Company v. Federal Power Commission*, 557 F.2d 349 (2nd Cir. 1977) (Prior administrative determination of whether interstate commerce would be affected by a new hydroelectric plant was not the same as the issue of navigability of the subject river, and thus the prior administrative determination would not collaterally estop a further administrative proceeding on the second issue); *Nasem v. Brown*, 595 F.2d 801 (D.C. Cir. 1979) (The absence of adversarial proceedings in the prior administrative decision did not provide the procedural safeguards necessary for the application of collateral estoppel in the latter administrative proceeding on the same issue).

[34]FAR § 9.407-2.

[35]*U.S. v. Alexander*, 743 F.2d 472 (7th Cir. 1984).

[36]Indeed, DoD Directive 5220.6, ¶ (f)(3), states the standard of review for security clearance cases. "Each personnel security determination must be a fair and impartial overall common sense decision based upon a consideration of all available information, both favorable and unfavorable, and must be arrived at by applying the standard that the granting (or continuance) of security clearance under this Directive may only be done upon a finding that to do so is clearly consistent with the national interest."

[37]Paragraph 14 of DoD Directive 5220.6 (Encl. 1) August 12, 1985 states:

> *Relevant and material oral, documentary, or other evidence may be received and technical rules of evidence shall be relaxed to permit the development of a full record. The Federal Rules of Evidence shall serve only as a guide.*

See also id., para 15 which states:

> *Records compiled in the regular course of business, or other physical evidence other than investigative reports, may be received and considered, subject to rebuttal without authenticating witnesses, provided that such information has been furnished by an investigative agency pursuant to its responsibilities in connection with assisting the Secretary of Defense, or the agency concerned, to safeguard classified information within industry pursuant to Executive Order 10865.*

[38]In the 1986 DISCR case against Lester Crown, a member of General Electric's Board of Directors and the holder of 23% of General Electric stock, defense counsel submitted affidavits from three former Secretaries of State, four Senators and two former Secretaries of Defense. *See* Novak, "Suspect," *Common Cause Magazine*, May/June 1989, at 20-21.

[39]DoD Directive 5220.6 (Encl. 1), para. 16, August 12, 1985.

[40]In the sample case, 8 months elapsed between the closing of the record and the issuance of the administrative judge's decision.

[41]DoD Directive 5220.6 (Encl. 1), para. 18, August 12, 1985.

[42]*Id.*, para 19.

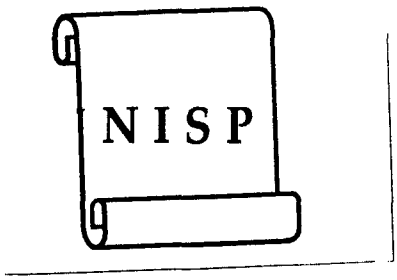
[43]*Id.*, para 20.

[44]Barton & Peterson, *Industrial Security Clearance Hearing: Heightened Importance a World of Corporate Acquisitions Takeovers and Foreign Investment*, 18 Public Contract Law Journal 392 at 408-409 (1989).

[45]5 U.S.C. Section 504, Pub. L. 96-481. effective October 1, 1981, as amended by Pub. L. 99-80, effective August 5, 1985.

[46]730 F.2d 1089 (1984).

[47]*Id.*, at 1092.



A Prudent Approach to Industrial Security: The Background and Promise of the National Industrial Security Program

Maynard C. Anderson*

The National Industrial Security Program (NISP) is a single, coherent and integrated Government security program with uniform, consistent standards and procedures for the protection of Government classified information held by industry. It mandates that all Government departments and agencies that contract with private companies to perform work requiring the use of Government classified information will protect that information in a uniform way and in accordance with a single Government regulation.

Origin and History of the NISP

The NISP is not an overnight phenomenon. The concept of a single industrial security program is the result of conferences and cajoling, of drudgery and dreams, of guidance and guile, of jockeying and jawboning, of probing and promises, of vision and visibility, of work and wisdom.

The Government[1] facilitated the process by which the NISP concept moved toward reality. Industry[2] was the catalyst that caused the interests and needs of all concerned to congeal into a single effort, the focus of which became improved, cost-effective security in industrial contracting.

Events leading to creation of a NISP took form as identifiable activities in the early 1980s when various Government and industry security officials began to express concerns about the process and effectiveness of safeguarding classified information held by industry. The concerns grew out of the increasing number of separate, conflicting, confusing and sometimes arcane regulations prepared by each Government department and agency for the protection of the same kinds of information. Documentation of circumstances began to emerge in which classified information was subjected to indiscriminate, inconsistent, repetitious, unnecessary, and even unworkable, security procedures at costs not commensurate with the risk of compromise. Informal discussions of the evolution of these situations among industry and Government officials over a period of years had not resulted in any significant progress toward improvement.

*The author notes with pride the many contributions by individuals and groups who provided inspiration with their ideas and then worked so long and hard to create the NISP.

*I also acknowledge the support of five dedicated security professionals whose assistance and comments on this article symbolize the cooperation among Government and industry officials that made possible the creation of a National Industrial Security Program.

*It would be impossible to describe even selectively the history and origins of the NISP without recognizing the valuable participations by Mr. Harry Volz, Director of Security and Transportation of the Grumman Corporation, and Mr. Jed Selter of the Boeing Corporation. Both as representatives of their respective corporations and as leaders of the Industrial Security Committee, Aerospace Industries Association of America, Inc., they persistently and relentlessly pursued the concept of a NISP. They were the driving force that brought together their industry colleagues, gained the support of other industrial associations, and inspired many in the Government to believe in a NISP. Without one, or the other, or both, there might not be a NISP.

I am particularly indebted to Ms. Rebecca A. Long, first for her accomplishments as the NISP Project Manager and Government Chair of the Monitoring and Evaluation Working Group, NISP Interagency Task Force; and second, for her research, collation of information and documents, and organization of much of the material information and documents, and organization of much of the material supporting this history. Grateful appreciation is offered also to Dr. Roger Denk, Director of the Defense Personnel Security Research Center (PERSEREC) and to Dr. Theodore Sarbin of the PERSEREC staff for their review, comments, and assistance in improving this recitation.

Because of the predominance of the Defense Industrial Security Program (DISP)[3] in industrial contracting by the Government, the Department of Defense (DoD) was clearly responsible for many of the situations and actions that led to the NISP concept. During the late 1970s and early 1980s, there began to emerge a specter that concerned the Director, Defense Investigative Service (DIS), the administrator of the DISP. His concerns centered around the proliferation of numerous special access programs (SAPs) protecting weapon system acquisition, many of which had diverse requirements and were "carved out" from inspection by the DIS. Some of these SAPs were created by renegade program managers who believed that the programs allowed more efficient operations. In fact, the SAPs imposed costly requirements on the contractors involved and hid from view possible security irregularities that would have been disclosed through regular, impartial inspections.[4]

In all fairness, some of these programs that controlled advanced technologies used to produce modern, sophisticated weapon systems were of benefit to the Government. They were outnumbered, however, by those of questionable value that appeared to be nothing more than a means to circumvent proper inspections and, sometimes, proper management.

In counterpoint, the DIS administration of the program was considered to be so structured, rigid, and inflexible that many program managers sought relief in provisions that allowed them to be exempt from regulations of the DISP.

Reports continued to circulate of large numbers of Government inspectors visiting the same facilities to look at the same things, and levying *ad hoc*, sometimes whimsical, requirements on their hosts. As a result and in the name of security, large amounts of money were spent to build unnecessary facilities, investigate personnel for high clearances and accesses of questionable need, and control information that was protected beyond its sensitivity.

These security anomalies did not go unnoticed and a concept for a single industrial security program was stimulated in 1982. The Secretary of Defense offered some ideas for a cooperative effort when he wrote:

> *We need industry to take the lead and inform both management and employees of the dangers (to our information security). In sensitive factories, we need voluntary security committees to safeguard essential designs and manufacturing know-how. Industry associations can play an important part in protecting our national security by advising member companies on appropriate measures and internal safeguards.*[5]

One of the objectives of the Secretary of Defense was to make certain that Western technology and productivity were not exploited to offset the chronic deficiencies of adversarial systems. Following the guidance of the Secretary, in talks to gatherings of industry officials that year I expressed the hopes that our future goals would include the application of resources to protect information that truly deserves protection; that methods would be devised to meet the diverse and changing environments in which information must be used; and that industry would play a larger role in assessing impacts of policy and give us advice as to the environmental adjustments that might be necessary to meet the threat.

"[The] concept for a single industrial security program was stimulated in 1982 [by the Secretary of Defense, who wanted]...to make certain that Western technology and productivity were not exploited to offset the chronic deficiencies of adversarial systems."

At its Spring meeting in April 1982, the Aerospace Industries Association of America (AIA) Industrial Security Committee provided me the opportunity to warn industry that "Your support is critical in stemming the flow of national security-related information to adversaries of the United States, and I have no doubt that we will be asking you and your chief executive officers for more assistance in the future to help us in that regard."

In May 1983, discussions at a joint meeting between the Government and the AIA continued in the context of anticipated changes in circumstances of contracting, of threat, of technology development and application, and of the adaptation of security policies and procedures to the results of

the probable changes. It was recognized that changes are not accomplished unilaterally, nor are they readily accepted by those comfortable with the *status quo* or who fear challenges of the unknown. Some of our colleagues reminded us of the writings of Ogden Nash in which he agonized that "Progress might have been all right once, but it has gone on too long."

During 1983, I ventured to tell some of the industrial groups concerned with security matters that neither Government nor industry could achieve the basic goal of proper protection of information without cooperation, coordination, and understanding as well as knowing as much as possible about the respective responsibilities, duties, and problems of the other.[6] When either Government or industry takes the position that the industrial security program belongs more to one than the other, and makes decisions arbitrarily without considering their impact and consequences, failure will likely follow.

The Harvard University Program for Senior Managers in Government makes the point that public objectives are not accomplished through direct production or delivery in the Government itself, but through other organizations whose conduct is influenced by the Government. So, Government and industrial constituencies, like those in the industrial security program, needed to consider carefully the kinds of influences that might be exerted by each other in order to determine the best opportunities for success. We concluded in 1983 that a much closer working relationship should be anticipated in the years ahead.

At a meeting of the National Security Industrial Association on February 28, 1984, specificity began to creep into my exhortations to industrial organizations when I suggested that:

> *Beginning at the earliest stages of negotiation, you must advocate the security procedures that you believe proper for contractual enterprises in which you are involved with the Government. You must share more of the technological burden of security. You will be required to develop yourselves, or share the risk of development at least with the Government, of systems that are mutually acceptable for security. You must support your proposals with proof that will be enhancing to your objectives, just as you should ask us why our changes will be beneficial. The time is coming when you and I must agree on what it is you must protect as a participant in the industrial security program, and you must then protect it as best you can. Micro-management by the Government will be impossible.*

At the AIA Industrial Security Committee meeting in May 1984, I offered the opinion, which I believe remains valid, that the roles and missions of Government and industry should be redefined, philosophically and actually, in order to respond with necessary flexibility to changes in requirements. I proposed decentralized operations with more centralized and coordinated controls in the industrial security programs. My argument included the hope that general security options would be developed applicable to all of industry in which policies and procedures would establish baselines and frameworks within which to work. I asserted that certain actions must be taken to make a NISP concept work. (See Figure 1.)

This time, the silence that characterized the response of our constituencies led me to wonder whether others really believed that better ways to do things must be found.

There had been little support at this point from any quarter for changes in industrial security policies or procedures. Much discussion and some hand-wringing continued over a state of affairs that was recognized as problematic, but progress toward improvement was not discernible.

Disagreement existed within both Government and industry as to what action could be taken, or how action might be taken, to relieve the effects on contractors of rigid and dogmatic enforcement of industrial security procedures on the one hand, and *ad hoc* requirements of multiple customers on the other. Some officials were loath to act because they relished the *status quo*. Others felt that everything was all right and, "if it ain't broke, don't fix it." Some wanted to abolish all SAPs as unnecessary, excessive, and costly. Some wanted to reform the industrial security programs, generally. And there were those in industry who believed that taking the initiative to offer program improvements would result in prejudicial criticism of their efforts, or even vindictive retribution against their firms or organizations by Government officials with authority over the programs concerned.

SPECIFIC ACTIONS RECOMMENDED TO AIA

Recognition that managing change equates to risk management, and protection will be selective.

Establishment of protection and resource priorities must be continuous. In conjunction with establishment of priorities, there must be identification and management of the commodities to be protected in terms of value, sensitivity, and potential damage regardless of storage media or characteristics.

Proper placement of responsibility for protection of information with the custodian. A continuing emphasis is required on the individual custodian and the relationship of various aspects of personnel security to personnel management. Managing change requires judgment and management in the true sense of the word at the lowest level of responsibility.

Uniform protection of classified information and critical technology in Government and industry.

Government and industry cooperation must be improved both on an institutional and individual basis. Some burden sharing between industry and Government must take place because an effective strategy will distribute and balance both the burdens and benefits of cooperation.

A free market utilization of available technology for security purposes. It is another fact, not an assumption, that we had better use technology because it will be used against us. Because we do not understand how something works doesn't mean that we cannot make use of it.

It must be demonstrated that security will contribute to income by preservation of an advantage to the nation as well as to the industrial enterprise -- a concept that has been called "beneficial cost."

Enforcement must follow cooperation with new methods like financial incentives and disincentives for security performance in contracts.

Security policies must be directed to vulnerabilities and real threats. They must accommodate the situation in the time and place applied. To manage changes, consideration of specific issues must be within the concepts of the program mission and objectives.

Figure 1.

Somewhat out of frustration, in February 1985, I told a meeting of the National Classification Management Society (NCMS) that we were developing a plan that would attempt to ensure that comprehensive and effective improvements were completed. The plan would utilize the resources and contributions of industry and Government based upon improvement of mutual understanding and reciprocal support. I invoked St. Augustine's admonition to teachers to "use what is already there" when I requested that we attempt to work together to develop a program that would not include policies that were beyond the comprehension of all, except experts in the field.

The text of my remarks to that NCMS gathering contained a plea:

> *I solicit your observations, conclusions and comments as to whether the needs of all parties concerned are being served properly by the structures in which you operate and by which you are served. These are not idle curiosities on my part. The* ***Harper Committee Report***[7] *observes that precise classification guidance is a prerequisite to the effectiveness of the information security program and can ensure that security resources are expended to protect only*

that which truly warrants protection in the interests of national security.

DoD leadership continued to offer support for improvement. To the AIA Industrial Security Committee in April 1985, I was able to offer a challenge from the Deputy Secretary of Defense, William Howard Taft, IV, who wrote in an internal memorandum to the Secretaries of the Military Departments and the Director, Defense Logistics Agency: "Seek out and challenge requirements and specifications that are not cost-effective." Applying his words to the industrial security programs, I concluded that we could not afford to deal with security in industry independently. Common, cost-effective solutions should be our goals. The design of a consistent, coherent concept of security in the context of the institutions involved must have the backing of those affected by the actions.

Slowly, during the mid-1980s, industry began to become more involved in industrial security policy formulation. Representatives of industry participated in both the Harper Committee and the Stilwell Commission.[8] They began independently to formulate positions that would lead to a single industrial security program. At the American Society for Industrial Security (ASIS) 34th Annual Seminar and Exhibits on September 28, 1988, I repeated what I had told the NCMS in June of that year: "It is necessary that you contribute to the future (program) with your judgments, advice, recommendations and management assistance."

To both the 1988 and 1989 Chief Executive Officer (CEO) fora,[9] I said

I will tell you without equivocation that we intend to exploit the private sector for advice concerning our successes and failures, as well as for systematic examination of problems and recommendations for improvements....If you present a consolidated position, you will have a significant impact on industrial security policy.

That comment brought considerable criticism from some industry representatives who believed that industry already spoke with one voice. Such was not the case, however, and as has become evident, when all the associations concerned with industrial security combine their voices, the much louder and unified expressions received more attention from the Government.

With the encouragement and support of several key Government officials, industry representatives intensified their efforts. Between March and July 1988 they generated several iterations of a white paper entitled "Toward a Rational Industrial Security Program." Despite the lack of widespread Government support, industry representatives were encouraged to document and develop supporting data for changes and to outline their ideas for a consolidated program.

On the basis of preliminary but unconfirmed data, industry began to build a plan for a single program and documented the number of conflicting and overlapping policies and redundancies while identifying associated costs for all security disciplines and programs.

"I invoked St. Augustine's admonition to teachers to 'use what is already there' when I requested that we attempt to work together to develop a program that would not include policies that were beyond the comprehension of all except experts in the field."

Concept Development

In March 1988, under the auspices of the AIA Industrial Security Executive Committee, security officials from a number of leading defense contractors and the Government began working informally on a program to standardize security practices within industry. The Industrial Security Committee of AIA approved continued project development. It was recognized that continuing top-level Government and industry support was critical to the success of the initiative. As earlier efforts to work within the system had failed, AIA executives, along with other industry officials, introduced the concept with a top down approach to CEOs and senior Government executives.[10]

During an AIA Industrial Security Committee meeting in May 1988, there was extensive discussion concerning possible form and substance of something like a NISP. Suggestions were advanced that the NISP should be codified in federal law, something that had been attempted during the

late 1960s without success. It was understood, too, that if the program was established by law, it could only be changed or modified by amendments to the law, a situation which would probably result in an unacceptably inflexible program. Conferees generally agreed that an executive order would probably be the most practical instrument of authority.[11]

On July 26, 1988, AIA representatives presented the details of a proposed NISP concept and strategies to me and the Director, DIS. Support and assistance to industry were offered along with our encouragement to continue concept development.

In August 1988, AIA sought involvement by the ASIS which committed active assistance. NCMS and the National Security Industrial Association (NSIA) also brought encouragement to the NISP initiative. Industry representatives began to accumulate data acquired through a survey of a limited number of member companies which provided evidence that security policies and procedural requirements generated independently by individual Government departments significantly increased costs without improving security.

To further support the belief that the problems identified in the earlier survey were not isolated, in 1990 AIA conducted an expanded survey[12] of some of the major aerospace companies to determine whether the security issues the NISP concept addressed were valid on a broader scale.

"[The November 1990 Cost Data Survey] highlighted a growing need for a consolidated program. It was a turning point in terms of gaining the attention, influence, and support from essential components of the Government."

Fourteen companies which derived a total of $32.8 billion annually from Government contracts responded to the survey. The fourteen companies employed a total of 340,000 cleared people and had almost twelve million classified documents, fifty-two percent of which were accountable[13]. This was a sizable survey to counter arguments of isolated problems and to gain support for more cost-effective security.

Five elements of existing industrial security programs were highlighted in industry's survey: Personnel Security, Security Briefings, Security Inspections, Physical Security, and Automated Information Security (hardware, software, facilities, and manpower). Key findings are highlighted in Figure 2.

SIGNIFICANT AIA SURVEY FINDINGS

- Fourteen Government agencies imposed 341 security regulations and directives on industry.
- Twelve Government agencies conducted multiple inspections at each facility (one contractor reported fifty-five inspections in one year requiring 442 man days of effort). One contractor reported 150 SAPs each requiring two annual inspections.
- One third, or 105,400 cleared employees, completed an average of eight sets of investigative forms for six different agencies.
- One third, or 105,400 cleared employees, required an average of seventeen separate security briefings.
- Industry's total reported cost from this survey was $.8 billion. It projected a $2 to $3 billion cost avoidance if duplication and redundancy with no added security protection could be eliminated through establishment of a single industrial security program.

Figure 2

The survey highlighted a growing need for a consolidated program. It was a turning point in terms of gaining the attention, influence, and support from essential components of the Government. Difficulty arose, however, when it became clear that such a program would mean giving up long-standing, traditional, and parochial practices. The need for standardized briefings, inspections, and universally accepted performance standards for industry was undeniable, but their achievement remained questionable. It would require each Government department and agency to accept each other's investigations, accreditations, and inspections, based on the same standards. Some Government agencies still held to the ideas that their programs were the best, and were working well.

The survey statistics, coupled with a diminishing funding stream, attracted interest in Government circles. From late 1988 until January 1990, AIA zealously kept up the pressure and continued to brief Government officials within DoD, the State Department, the Central Intelligence Agency (CIA), the Department of Energy (DOE), the Federal Bureau of Investigation, and others.[14] Government officials expressed enthusiasm and many offered their support. A briefing was held for Lt. Gen. Brent Scowcroft, USAF (Retired), Assistant to the President for National Security Affairs, in November 1989. He recited personal frustrations resulting from having repeatedly to complete investigative forms despite his long years in the service of his country. He commented favorably on the merits of such a program and challenged industry to continue briefing the concept to key Government executives.

In December 1989, shortly after the briefing of General Scowcroft, Dr. Robert Gates, then Assistant to the President and Deputy for National Security Affairs, requested that other members of the National Security Council be briefed on the concept.

By early 1990, most Government executives in Washington who were in a position to influence and create change in Government programs, had been briefed. Briefings, speeches, and symposia involving industry and Government representatives, all extolling the virtues of a NISP, intensifed in noise and number.

In March 1990, General Scowcroft and Dr. Gates both corresponded with the President of AIA expressing appreciation for industry's efforts concerning the NISP. Lieutenant General Scowcroft noted that "codifying industrial security procedures under a NISP are of vital importance....We continue to have the concept under active consideration within the Government." Dr. Gates added that "the NISP concept is an excellent example of what can be accomplished if industry and Government work together on problems of mutual interest."

The President Acts

Industry had provided documentation to support its position on the need for a NISP. Now a Government review was required formally to develop information on the issue.

On April 4, 1990, President Bush signed a National Security Review entitled "The National Industrial Security Program" in which he directed a review of the Government's industrial security programs to determine the feasibility of establishing a single program applicable to all Government departments and agencies. He further directed the Secretary of Defense to take the lead and coordinate efforts with the Secretary of Energy and the Director of Central Intelligence.

The President's direction was specific and detailed as to what the review should cover. He asked for answers to the following questions:

— How can we standardize security training?

— Can we develop uniform inspection compliance standards?

— What single set of baseline standards can we develop applicable to all Government agencies and departments?

— Should there be layered security controls?

— What should be industry's role in the NISP?

— What shifts in priorities and resources are needed to effect a NISP?

— What changes are needed to improve security effectiveness and ensure cost efficiency?

— Which agencies and departments should develop standards and procedures and who should have oversight responsibility?

NISP Phase I--Government Review

The Secretary of Defense delegated responsibility for the NISP review to the Under Secretary of Defense for Policy.[15] As the Assistant Deputy Under Secretary of Defense (Counterintelligence and Security), I initiated the review on April 19, 1990.

A NISP Project Manager was named who began to develop a plan of action. We established a working group with representation from all Government departments and agencies who have sizable industrial security programs.

Six Government agencies (State, Treasury, Energy, the Nuclear Regulatory Commission, the Attorney General/Federal Bureau of Investigation and the Central Intelligence Agency) and thirteen DoD agencies (the Joint Chiefs of Staff, the Strategic Defense Initiative Organization, the Defense Investigative Service, the Defense Intelligence Agency, the Defense Logistics Agency, the Defense Mapping Agency, the Defense Nuclear Agency, the Director of Advanced Research Projects

Highlights of Government Survey Findings

- The Government has more than 15,000 cleared contractor facilities employing more than 1.5 million cleared contractor employees.
- Various rules and regulations implement or supplement the basic executive orders and legislation. They include 47 different standards, manuals and directives that create a significant regulatory burden to industry and Government.
- Various agencies sponsor programs designed to maintain threat awareness in industry. Virtually all agencies and departments of Government have security awareness training programs, briefings, and materials available for use by their contractors but they are all poorly utilized.
- A lack of uniform personnel security requirements and reciprocity of investigations throughout the Government cause unnecessary costs as a result of redundant investigations and lost time while personnel wait for clearances.
- Special activities (Sensitive Compartmented Information (SCI), SAPs, and Energy/Restricted Data (E/RD)) and programs should have supplemental controls only if it has been determined that baseline security programs do not provide adequate protection.
- Security oversight of industry is applied inconsistently by Government agencies with generally no reciprocity for facility accreditations, certifications, or inspections among agencies and departments.
- Most departments and agencies have no mechanism for determining the costs of the industrial security program. They noted that security costs are generally embedded in other program elements. When estimates were provided, they seemed low. There were no means available within the Government for validating and separating security costs from other program costs.

Figure 3

Agency, the National Security Agency, the Army, Navy, Air Force, and the Secretary of the Air Force for Space Systems) participated in the review. During the Government review, industry was kept abreast of developments through continuing coordination among industrial associations and the review coordinator.

A survey questionnaire, designed to elicit some of the same kinds of information as that documented by the earlier industry survey, was developed and provided to the six Government departments and agencies as well as the thirteen DoD agencies participating in the review. The Government review produced information that convinced many more Government officials that changes were needed. Findings summarized in Figure 3 revealed data that were heretofore unknown or not publicized.

The Government survey provided a reported total estimate for industrial security of $241.6 million by participating DoD and other Government departments and agencies. (Because of accounting methodologies in industry, it was concluded that industry's total estimate of $.8 billion was somewhat more supportable than the scattered figures from the Government departments and agencies.) Since the estimates reported were low (the security for the B-2 alone was well in excess of $241.6 million), indirect program costs to the Government were developed and calculated by extrapolating industry-reported costs to the total number of personnel and cleared facilities in the program for each cleared employee. The total estimate was $13.8 billion.[16]

Evidence was acquired during this review which confirmed the Government's use of multiple rules to protect information of the same sensitivity, inconsistent application and enforcement of those rules, and an inability to determine program costs.

Response to the President

The report to the President[17] following the initial program review indicated that the concept of a national program for security in industry was feasible and desirable. Moreover, the Secretaries of Defense, Energy, Treasury, the DCI, the Attorney General, and the Chairman, NRC, all generally supported the concept of a single integrated system of industrial security for classified programs. The report also contained the general consensus of both Government and industry representatives that SCI, SAPs and energy-unique activities should be subject to supplemental controls.

The report proposed that an Interagency Task Force led by the Secretary of Defense, the DCI, and the Secretary of Energy, with industry participation, would design a national industrial security program to be implemented under the general oversight of the Executive Office of the President.

The President Concurs

On December 6, 1990, the President concurred in the plan provided by the Secretary of Defense and supported by the DOE and DCI. He directed that a task force develop elements of a NISP as outlined in the report. The President further requested that recommended policy changes be provided to the National Security Council by September 1, 1991.[18]

NISP Phase II--Joint Government-Industry Review

As the Assistant Deputy Under Secretary of Defense (Counterintelligence and Security), I was again designated the responsible official for leading and directing Phase II of the NISP. A plan of action, goals, and strategy for establishing the Interagency Task Force were created. Our goals are set forth in Figure 4.

Representatives from Government departments and agencies, along with industry delegates who participated in the phase I review and others, attended the first planning and organization meeting of the task force on January 22, 1991. We formally established the task force that day. It consisted of the Executive Committee, Steering Committee, and ten Working Groups. The Steering Committee was directed to report to the Executive Committee, members of which had departmental or agency program approval authority for their respective departments. An eleventh working group, the Monitoring and Evaluation Group, was established to serve as the focal point for all activities and to provide support to the Steering Committee. I served as the Defense official responsible for directing and overseeing completion of program development and co-chaired the Steering Committee with an industry representative, Mr. Harry Volz, Director of Security and Transportation, Grumman Corporation.

We also developed and accepted a plan for the task force and a program for accomplishing the President's goals that same day. Our plan outlined an organizational structure and strategy for achieving program development, organization and planning for the task force, and the establishment, authority, regulation, baseline, and supplemental components of a NISP. The plan also included milestones and timetables for completing each task.[19]

Some of the guidance for the task force and working groups was derived from Deputy Secretary of Defense Donald J. Atwood, who, when speaking generally about regulatory review on October 4, 1989, directed that issuances should be clear and assume that those responsible for their implementation down to the operating level are competent, trained, and want to do a good job. He added that the need for a policy procedure or requirement must clearly add value to our fundamental mission, and that issuances should be written in such a way that supplementation by the military departments will be the rare exception rather than the rule.

The division of labor among the working groups was designed so that each would concentrate on a separate security discipline. In some cases, like that of the Information Security Working Group, it was determined desirable to form subgroups to deal with the clearly separate areas of SAPs, SCI, and energy-related programs. Formulation of the working group dealing with threat was a product of the first meeting on January 22. Initially, consideration of the threat was concluded to be a requirement of each group as it worked to develop its own policies. The consensus of the entire task force, however, resulted in formation of a separate working group on threat that would attempt to determine not only changing threats as they affect policy formulation, but improved means of communicating the threats to industry.

GOALS OF THE NISP INTERAGENCY TASK FORCE

- Conduct a comprehensive regulatory review.
- Develop an instrument of authority for a single industrial security program.
- Develop and promulgate uniform standardized security policies.
- Establish a mechanism for determining complete industrial security costs.
- Ensure completion of ongoing personnel security initiatives for a single scope background investigation applicable to all Government departments and agencies.

Figure 4

"Deputy Secretary of Defense Donald G. Atwood... directed that [regulatory] issuances should be clear and assume that those responsible for their implementation down to the operating level are competent, trained, and want to do a good job....[Any proposed] policy procedure or requirement must clearly add value to our fundamental mission, and... supplementation by the military departments will be the rare exception rather than the rule."

Formation of the working group on threat and creation of the Monitoring and Evaluation Working Group were two of the first formal examples of the ability of a combined group of Government and industry representatives to achieve consensus on issues related to a NISP.

The working groups functioned as teams to design the future program elements, beginning with basic policies and proceeding to details that would provide the functional guidance to implementers. This concept allowed the formulation of segregable policies, or elements, that could be approved and implemented immediately despite what might happen to the NISP in its entirety.

Industry, Government, and all affected communities[20] were involved in the working groups and the Steering Committee. Each working group was headed by a Government and industry co-chair. The infrastructure of the task force was designed so that participants could immediately consider and coordinate proposals among all equity holders. The anticipated collaboration was expected to stimulate innovation and creativity. At the initial meeting, all participants were advised that there were no pre-

conceptions as to what the final program might look like, and the process could begin with "a clean sheet of paper."

It was discovered subsequently that the "clean sheet of paper" approach was not viable. Most members of the intelligence and security community have been shaped by training and experience so that they are more comfortable dealing within a framework of established mechanisms and rules. It is much easier to change policies by tinkering than it is to achieve revolutionary change from the ground up. Through the cooperative mechanism that was being established, however, it was hoped that standards could be developed that would provide motivation for all participants to improve the effectiveness of their respective organizations, particularly as implementation of the NISP began.

Because of the diversity of the experience and qualifications of members of the various working groups, and some reluctance on their part to start from scratch, it was decided that the Regulatory Working Group and each working group would review current policies and procedures, *in toto* and by subdiscipline, respectively, in order to preserve that which works well and which would presumably work well in the future. The preserved elements of current policies and procedures would then serve as the foundation for new innovative elements that would complete the requirements for a program.

The task force structure was designed to integrate the policy-making structures of the Federal Government security community to the greatest extent possible. For example, the Director, Information Security Oversight Office (IS00), who has responsibility for information security in the Government and is Chair of the Information Security Committee, Advisory Group/Security Countermeasures (AG/SCM), agreed to serve as the Government Chair, Information Security Committee, NISP Task Force. Likewise, the Director of Security, CIA, who is the Chair of the Personnel Security Committee, AG/SCM, agreed to serve as the Government Chair, Personnel Security Committee, NISP Task Force. They both also serve as members of the NISP Steering Committee.

The Director, Security Plans and Programs, DoD, in his capacity as Chair of the National Industrial Security Advisory Committee (NISAC), was named Executive Secretary of the Steering Committee. He was then also the DoD Member of the DCI Security Forum, the Chair of which is also a Steering committee member. A representative of industry is a delegate to the NISAC. Since I served as the Chair, AG/SCM, as well as the Chair, NISP Task Force, there were continuing opportunities to ensure that policies affecting security in general that were under consideration in other fora would be compatible with those proposed for inclusion in the NISP.

Members of all of these other groups frequently served as members of appropriate NISP working groups, so redundant and repetitious discussion and debate was often eliminated and issues brought to closure more quickly than if they were independently considered in each of the many groups and committees.

Two principal examples of greater efficiency in Federal policy making have emerged from the NISP process. First, a single scope background investigation (SSBI) for access to Top Secret and SCI was under consideration in the AG/SCM and the DCI Security Forum for a number of years. When directed by the President, the single scope BI became an objective of the NISP task force also. Agreement concerning its requirements was achieved with relative speed after all parties coordinated their discussions in the various fora and forwarded a recommendation to the National Security Council. This action resulted in a National Security Decision by the President on October 21, 1991. It is also an example of the development of a segregable element of policy.

The other example involves the review of Executive Order 12356, "National Security Information." The National Security Council directed a review of this Order by the Director, ISOO, prior to the President's direction to review the industrial security programs of the Government. The mission of the industrial security program is to protect classified information loaned to industry to allow performance on contracts. It seemed to make sense to include the authority for the industrial security program in E.O. 12356, and to combine the review of that Order with formulation of policy for the NISP. One executive order designed to cover the entire information security program would eliminate the necessity to coordinate the preparation of two orders, or one order and another instrument of authority establishing the NISP, throughout the various Government departments and agencies. Further, Congress historically has taken a keen interest in provisions of the Executive Order that deal with the protection of classified information,

and it seemed desirable to have Congressional interest focus on these proposed provisions once rather than twice. The provisions of the other Executive Order dealing with personnel security of contractor employees (E.O. 10865) would remain unchanged; therefore, its reissuance should attract no particular attention. This method of dealing with the review of E.O. 12356 has seemed to be both an efficient and effective means of establishing authority for a NISP while modernizing information security policy in general.

I previously noted that the working groups were established to deal with discrete security disciplines. A notable exception to that is the Regulation Working Group which must cross all security disciplines as it works toward its objective of establishing a single regulation. That regulation, to be called the *National Industrial Security Program Operations Manual* (NISPOM), will include the set of rules by which the NISP will function. Other working groups will feed the Regulations Working Group with the necessary information and material to establish the rules. The other exception to the general premise is, of course, the Monitoring and Evaluations Working Group, which was established to ensure that the efforts of all the other working groups were coordinated and directed toward completion of the basic mission.

Working group chairpersons were selected by the Steering Committee. Chairpersons were responsible for creating their own groups, preparing terms of reference by which to operate, ensuring representation from appropriate Government departments and agencies and from industry, and establishing an agenda. The charters and objectives of each group were formalized and submitted to the Steering Committee for approval.

By late March 1991, most working groups were well into the effort, and on 2 May 1991, the Steering Committee provided an interim report to the Executive Committee.[21] The report depicted the task force organization, outlined NISP initiatives, and provided a summary of accomplishments. The report confirmed support by all committee members for establishing a single program for industry. Phase II accomplishments are listed in Figure 5.

Phase II Report to The President

The September 1991 Report to the Presidents advised that the NISP had been accepted by Government and industry officials and the Task Force had successfully developed the critical components of the NISP. Supplemental standards were included for SCI, SAPs, and Energy/Restricted Data programs. The report advised that oversight organizations and responsibilities for the NISP would utilize existing offices, departments and agencies and assign to them the responsibilities for the NISP, eliminating the need to create a new organization for oversight purposes. The concept of minimum standards for security had been abolished. Stated standards would be the only standards. The report further affirmed preservation of the responsibilities of the Secretaries of Defense and Energy, the NRC, and the DCI that are derived from their statutory and Presidentially delegated authorities.

The report included a critical path for the next and succeeding phases which outlines significant events and important timelines by which full implementation of the NISP can be realized by the end of 1995. The Steering Committee outlined the needed actions through 1995 and noted that the majority of other changes could be implemented by the end of 1993.

The President Responds to Phase II Report

On January 29, 1992,[23] the President noted in a memorandum to the Secretary of Defense that "The Government-industry task force you established has made considerable progress toward development of a single, coherent, and integrated program. This remarkably collaborative effort between Government and industry will lead to significant improvements in the security of our Nation." The President continued, "I am especially pleased with the projected time frame in which you intend to fully implement this vital program, which will provide cost-effective and secure development and delivery of systems essential to our national security."

The Future

Industrial security is part of public policy. The NISP is a collaborative effort by Government and industry that has attempted to measure the impact of Government policies in terms of benefits and costs: present and future, affordable and avoidable. The NISP, in its imposition of requirements, has environmental consequences as a result of physical requirements. It involves human resource

PHASE II ACCOMPLISHMENTS

- An instrument of authority for the NISP, a proposed executive order with its implementing directives, near completion
- A Single Scope Background Investigation approved; development of a uniform personal history form in progress
- Threat and value driven, cost effective standardized security policies and requirements for the physical protection of sensitive assets and collateral, SCI, and SAP information underway
- Protective measures based on consideration of updated counterintelligence and operational security analyses of the existing threat as well as the vulnerability and value of the asset
- Standards, policy, and training requirements for the physical protection of sensitive assets and collateral, SCI, and SAP information underway
- The Director, ISOO, designated as the most likely responsible official for implementing and monitoring the NISP. The Secretary of Defense to serve as executive agent and the Secretary of Energy, the NRC, and the DCI to be responsible for the administration of matters and operation of programs under their authorities as part of the NISP
- The NISP Advisory Committee, under the chairmanship of the Director, ISOO ,would provide the mechanisms for policy changes and resolving issues
- Agreements among inspecting agencies at contractor facilities involving multiple contracts to be reached to minimize the number of inspections
- A *NISP Operating Manual* to serve as the single regulatory standard for the NISP
- Security education and training programs and requirements developed. As NISP implementation proceeds, requirements to be identified
- Individual departments and agencies responsible for implementing the procedures of the NISP, including reallocation of resources through the budget process, as soon as possible after the executive order and applicable directives are promulgated
- A methodology for identifying Government and industry costs associated with industrial security programs
- NISP utilizes existing offices, departments and agencies and assigns to them responsibilities for the NISP

Figure 5

implications as a result of investigative intrusions into the backgrounds of organizations and individuals, along with adjudicative decisions concerning them. The NISP also exerts influences on business decisions in terms of general competition as well as foreign investment in United States companies with classified contracts. It has an impact on the sharing and control of technologies, their future uses for the benefits of the Government and civil communities. And, above all else, it has continuously reinforced in all of the participants in its formulation, a devotion to its primary purpose: improving the national security of the United States.

The NISP lays the foundation for broader opportunities to provide academic support to the professional security officer both in industry and Government. The DoD, Michigan State University (MSU), and industry have undertaken a program of instruction and research at the graduate and un-

dergraduate levels with emphasis on the NISP. In addition to degree programs in security management, MSU will also provide security professionals with advanced study and research opportunities through creation of a center for security leadership and management. The program will enhance all professional aspects of every security discipline as well as contribute to more informed policy decisions through rigorous research and study.

I believe the NISP will be a catalyst for significant changes in how the Government does business in security in the future. In addition to those it has already inspired, it will produce other major changes in information security, personnel security, physical security and international security that will influence all of the cultures affected by security.

The phase of the NISP dealing with development of policies has nearly concluded. It seems as if a reasonable blueprint has been prepared. Building the procedures and their implementation will prove its worth. Hopefully, its future stewards will accept it as a living program, the care and feeding of which will serve us well for a long time.

The NISP project may have been the first and only cooperative Government and industry effort of this size to achieve early and rapid success in making improvements to a major Government institution. I hope General Scowcroft was right when he ventured that the NISP initiative can and should be used as a model program by which the Government, collectively and working jointly with the private sector, can find solutions to other modern problems.

Maynard C. Anderson is the Assistant Deputy Under Secretary of Defense for Security Policy

FOOTNOTES

[1]Government here refers to the representatives of all Executive Branch departments and agencies participating in developing the NISP, principally the Department of Defense, Department of Energy, and the Central Intelligence Agency.

[2]Industry is an all-inclusive term that refers both to representatives of industrial contractors and the major organizations that represent their interests in matters of industrial security: The Aerospace Industries Association of America, Inc.; The American Society for Industrial Security; the National Classification Management Society; and the National Security Industrial Association.

[3] Over a period of many years, the Department of Defense developed a comprehensive industrial security program to safeguard classified information released to industry. The authority for the DISP is Executive Order 10865, "Safeguarding Classified Information Within Industry," February 20, 1960, as amended by Executive Order 10909, January 17, 1961.

[4]SAPs may be created only by designated Agency Heads pursuant to Section 4.2 of Executive Order 12356, "National Security Information," April 2, 1982. The criteria for establishing SAPs are: (a) normal management and safeguarding procedures do not limit access sufficiently to the nation's most sensitive national security information, and (b) the number of persons with access is limited to the minimum number necessary to meet the objectives of providing extra protection for the information. As defined by DoD Directive 0-5205.7, "Special Access Program (SAP) Policy," January 4, 1989, a SAP is, "Under the authority of E.O. 12356...and as implemented by the ISOO Directive No. 1...any program created by an Agency Head whom the President has designated in the Federal Register to be an original TOP SECRET classification authority that imposes "need-to-know" or access controls beyond those normally required by DoD Regulations for access to CONFIDENTIAL, SECRET, or TOP SECRET information." Prior to issuance of this directive, SAP creation and oversight in the DoD was controlled inconsistently.

[5]Secretary of Defense Caspar W. Weinberger in *The Wall Street Journal*, January 12, 1982.

[6]Maynard C. Anderson remarks to meetings of the ASIS, March 25, 1983, and the AIA Industrial Security Committee, May 17, 1983.

[7]The Harper Committee Report was a report to the Deputy Under Secretary of Defense for Policy by the Department of Defense Industrial Security Review Committee (December 1984), which contained an analysis of the effectiveness of the DoD Industrial Security Program and offered recommendations for program improvement. The committee was convened as a result of the arrest of James Durward Harper, Jr., for alleged espionage activity involving a DoD contractor facility, and it was from him that it obtained its name.

[8]The so-called Stilwell Commission, named in honor of its chairman, General Richard G. Stilwell, USA (Retired) (1917-1991), was established by the Secretary of Defense as the DoD Security Review Commission in the wake of arrests of three retired and one active duty Navy member on charges of espionage. The Commission was directed to conduct a review and evaluation of DoD security policies and procedures and identify any systematic vulnerabilities or weaknesses in the programs. It produced a report on 19 November 1985, *Keeping the Nation's Secrets.*

[9]CEO Forum, November 9, 1988, Lockheed Corporation, Calabassas, California and CEO Forum, July 10, 1989, Grumman Corporation, Bethpage, New York, were convened by the Deputy Under Secretary of Defense for Policy in order that CEOs, their Security Directors, and representatives of the government could discuss the effective management of security in industry. Results of the Forum at Grumman Corporation were recorded on video tape and may be available for review with permission of that firm.

[10]Chronology of NISP concept development, coordination and implementation by Jed Selter, Boeing Corporation, June 1, 1991 rev.

[11] There were reports following this meeting that I had stated, in public session, that a NISP would never happen. I do not recall it, but if I made such an intemperate statement, subsequent events have hopefully proved it to be merely a quickly passing lack of faith.

[12] Appendix C (AIA Cost Data Survey) to "A Report to the President by the Secretary of Defense on the National Industrial Security Program," November 1990.

[13] "Accountable" generally refers to that information classified Secret and above controlled by a system of records that assures the documentation and tracking of the information in whatever media.

[14]Chronology of NISP concept development, coordination and implementation by Jed Selter, Boeing Corporation, 1 June 1991 rev.

[15]Secretary of Defense Memorandum, Subject: "The National Industrial Security Program (NISP)," October 17, 1990, delegated authority to the Under Secretary of Defense for Policy to act on his behalf for the development, execution, and management of the NISP.

[16]NISP survey.

[17]A Report to the President by the Secretary of Defense, "The National Industrial Security Program," November 1990.

[18]President's Memorandum to the Secretary of Defense, December 6, 1990.

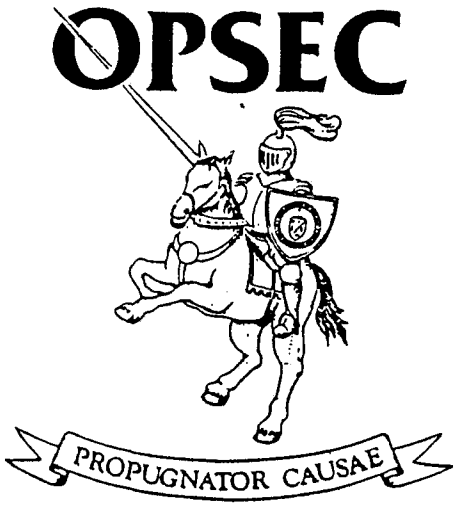
[19]NISP Planning and Organization Meeting Minutes, January 22, 1991.

[20] The term "communities" refers to groups of like organizations, or organizations with related missions and functions, *e.g.*, the Intelligence Community.

[21]NISP Steering Committee Interagency Task Force Status Report on the NISP, 2 May 1991.

[22]"The National Industrial Security Program - A Report to the President," September 1991.

[23]The President's Memorandum to the Secretary of Defense of 29 January 1992 on the National Industrial Security Program.



KURT'S LAWS OF OPSEC

Kurt W. Haase

INTRODUCTION

Intelligence collection and analysis are very much like assembling a picture puzzle. Each piece of the puzzle could be an item of information that is not classified or an indicator by itself but, when assembled with other pieces of the puzzle, could damage national security by inadvertently revealing classified or sensitive unclassified information regarding programs, activities, and capabilities.

Concerns over the inadvertent compromise of classified information or the loss of sensitive unclassified information led to the development of a National Security Decision Directive establishing a National Operations Security (OPSEC) program.

The goal of OPSEC is to make hostile intelligence-gathering more difficult and time consuming. The longer it takes for an adversary to acquire our national secrets, the longer our nation can maintain its military and technological edge.

OPSEC *as a methodology* originated during the Vietnam conflict when a small group of individuals, operating under the nickname Purple Dragon, was assigned the mission of finding out how the adversary had been obtaining advance information of certain combat operations in Southeast Asia. Although traditional security measures provided the physical protection of classified information, a new approach was needed to deal with all of the unclassified indicators that could be pieced together to derive critical operational information.

The Purple Dragon team conceived the methodology of analyzing U.S. operations from the perspective of the adversary. The team was successful in what they did and, to name the methodology used, they coined the term Operations Security.

The Interagency OPSEC Support Staff, or IOSS, published a booklet entitled "The Great Conversation," which was written by Ron Samuelson. He was a member of the original Purple Dragon team and was responsible, in part, for coining the term operations security. It is not my intent to go into the history of OPSEC, since the IOSS publication provides an excellent summary.

What I would like to point out, however, is that those early methods and techniques have been modified and improved over the years by OPSEC professionals. Furthermore, it is now recognized that the OPSEC methodology is applicable in virtually every Government program that has information requiring protection.

Implementing an OPSEC program cannot be achieved without first establishing a program foundation. This requires appointing an individual to be responsible for the overall management and administration of the program, the OPSEC manager. It also requires defining what is to be achieved and how it is going to be achieved, the OPSEC plan. The plan designates knowledgeable, experienced personnel from major elements of the organization to assist the OPSEC manager, the OPSEC working group. Finally, the manager must develop program files for reference and program documentation.

Once the program foundation has been established, all members of the organization should become OPSEC aware. They must understand the OPSEC process and their role in preventing the exploitation of information.

To provide a simplified understanding of the OPSEC process, I have developed three Laws of OPSEC and an OPSEC Maze that reduce the process to the basic fundamentals of understand-

ing the threat, recognizing what information is to be protected, and protecting information from exploitation.

KURT'S LAWS OF OPSEC

Let us start with Kurt's Laws of OPSEC, Figure 1.

Kurt's first law of OPSEC: "If you don't know the *threat*, how do you know *what* to protect?

If there were no threats to our programs, activities, facilities, personnel, or information, there would be no requirement for gates, access control procedures, access clearances, classification, and so forth.

However, as security managers or OPSEC professionals, we recognize that threats do exist, although specific threats may vary from site to site or from program to program. Therefore, we must document, in a site-specific statement of threat, the actual and postulated threats. Generic threat examples might include:

- Nuclear Proliferant(s)
- Foreign Intelligence Collector(s)
- Criminal(s)
- Terrorist(s), and
- The Insider(s).

In any given situation, there is likely to be more than one adversary, although each may be interested in different information.

For example, a terrorist may be interested in information about the movement of a nuclear device for the purpose of theft or sabotage, whereas a foreign intelligence collector may be gathering information to determine the final destination of the device or to determine the number of devices in our inventory.

An adversary's ability to collect, process, analyze, and utilize information must also be determined. The objective is to know as much as possible about each adversary and the strategies available for targeting the organization.

Now that we have identified the threats, we consult Kurt's second Law of OPSEC: "If you don't know *what* to protect, how do you know you are *protecting* it?"

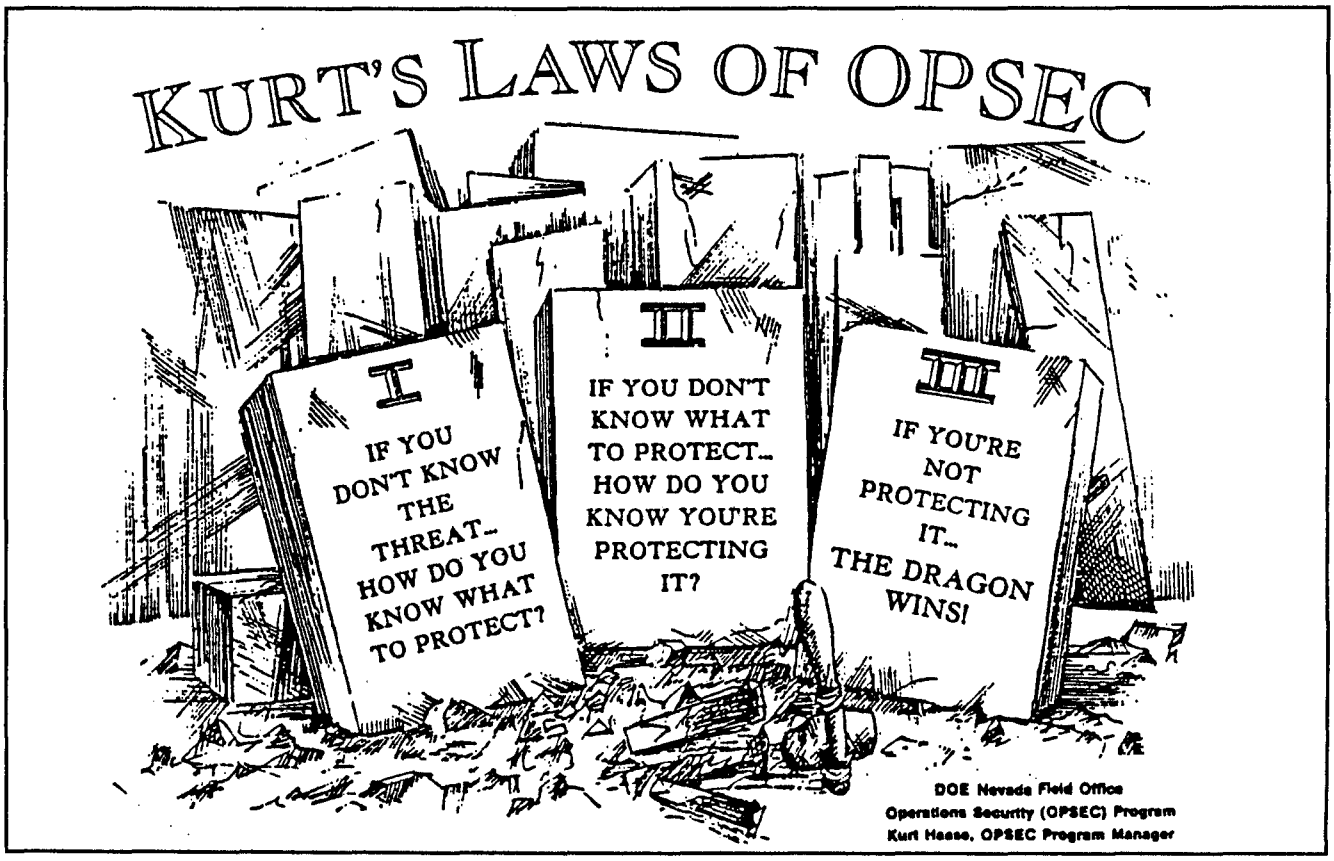


Figure 1

The "what" is the critical and sensitive, or target, information that adversaries require to meet their objectives. Critical and sensitive information need not be classified.

Critical and sensitive information may be determined by answering the question: "If I were a (insert a specific adversary), what would I want to know?"

This question must be answered from the perspective of each identified adversary.

When critical or sensitive information is determined, it is entered onto a master list called a Critical and Sensitive Information List or CSIL.

Generic examples of target information may be:

- Long-term plans
- Production quantities
- Material movements
- Date of a test and test results
- Protective force capabilities and vulnerabilities
- Certain aspects of work-for-others, or
- Material inventory

In the next step it is important to understand the premise of OPSEC: The *accumulation* of several elements of *unclassified* information could damage national security by revealing classified information.

The *detectable activities* and *bits of data* that can be pieced together to derive the critical and sensitive information are called Essential Elements of Friendly Information or EEFIs.

EEFIs are the pathways, indicators, or open source information that, when collected and analyzed by an adversary, could reveal target information.

As I have mentioned, information of intelligence value is collected from many sources. These sources could include:

- Intelligence debriefing following a visit to a facility
- Intercepting FAX communications
- Analyzing news articles
- Monitoring budget information of an organization
- Monitoring travel of key personnel
- Reviewing position vacancy announcements
- Sifting through the organizations' unclassified waste
- Analyzing publications, journal articles, and other open source documents
- Analyzing procedural manuals

Eventually, significant information (EEFIs) could be assembled that would reveal the target information (CSIL).

EEFIs are identified by answering the question: "If I were a (insert adversary), how or where would I go to obtain the information?" Typically, the individual pathways or indicators are considered unclassified and are often beyond the purview of traditional security programs even to identify, let alone classify and protect.

Generic EEFI examples might include:

- Environmental impact statements
- Various reports, such as monthly, annual, quarterly
- Meeting minutes or notes
- Work schedules
- Purchasing requests
- Scope-of-work orders
- Travel requests/trip reports
- Progress reports
- News releases
- Published articles
- Corporate newsletters
- Patents

Because information that may be of value to one adversary may not necessarily be of value to another adversary, EEFIs must be identified from the perspective of *each* adversary.

Thus far we have identified *threats* and we have determined what information we want to protect. Now we turn to Kurt's third law of OPSEC: "If you are not protecting it (the information),... *THE DRAGON WINS*!"

We determine whether or not we are protecting our critical information by conducting what are called OPSEC vulnerability assessments (sometimes referred to as just OPSEC assessments).

An OPSEC assessment is a critical analysis of what we do and how we do it from the perspec-

tive of an adversary. Activities are assessed to identify exploitable indicators. Internal procedures and information sources are also reviewed to identify possible inadvertent releases of information. Open source information that can be interpreted or pieced together to derive critical information must also be analyzed.

Quality OPSEC assessments require time, patience, and the cooperation of personnel. Therefore, OPSEC assessments should be:

- Fact finding, not fault finding
- Not compliance-oriented
- Non-attributable

Members of my OPSEC assessment team may include:

- Nevada contractor or laboratory representatives
- Representatives of the National Security Agency
- The Federal Bureau of Investigation
- The Air Force Electronics Warfare Center
- The local Army military-intelligence detachment
- Others, depending upon the scope of a particular assessment.

If, as a result of an OPSEC assessment, it is determined that one or more EEFI items are exploitable by an adversary, we have identified an OPSEC concern or a vulnerability.

Vulnerabilities and specific threats must be matched. Where the vulnerabilities are great and the adversary threat is evident, the risk of adversary exploitation is assessed as high. Therefore, a priority for protection needs to be assigned and corrective action taken.

Where the vulnerability is slight and the adversary has a marginal collection capability, the priority is usually considered to be low.

Once OPSEC concerns or vulnerabilities are identified, countermeasures must then be developed and implemented in order to protect the information from exploitation, or at least to make the collection capability more difficult for the adversary.

Once countermeasures have been taken, they should be reviewed periodically to evaluate their effectiveness.

In order to track our OPSEC assessments and recommendations at the Nevada Field Office, we have developed a tracking database. Each recommendation has a specific identification number assigned to it. Information can be retrieved from the database by the specific recommendation number, by date of assessment, by organization conducting the assessment, or by type of vulnerability.

OPSEC MAZE

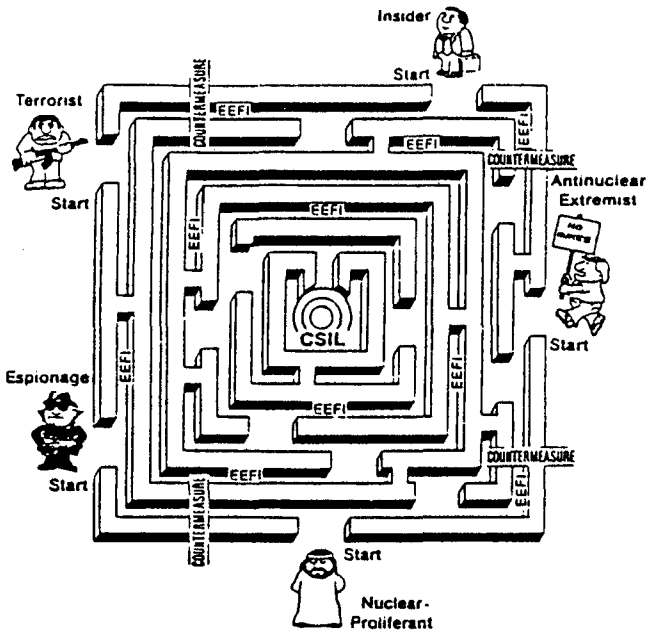


Figure 2.

THE OPSEC MAZE

I developed the OPSEC Maze to illustrate the relationship between the threat (Kurt's first law of OPSEC); critical, or target, information (CSIL) as well as pathways and indicators (EEFIs) (Kurt's second law of OPSEC); and countermeasures (Kurt's third law of OPSEC).

Figure 2 shows how the laws operate. On the perimeter of the Maze are several generic adversaries, or threats; (Refer to Kurt's first law of OPSEC.) Note that each adversary has a different starting point. This is to indicate that, in any given situation, there is likely to be more than one adversary, although each may be interested in acquiring different information.

The OPSEC Maze contains pathways, or indicators (EEFIs), leading to the target information

(CSIL). (See Kurt's second law of OPSEC.) Note, again, the different pathways to indicate that a particular EEFI that is important to one adversary may not (necessarily) be important to another adversary.

Throughout the OPSEC Maze are barriers or countermeasures that have been implemented in order to prevent compromise of critical information- (The point of Kurt's third law of OPSEC.)

DOE NEVADA FIELD OFFICE OPSEC AWARENESS PROGRAM

Upon reviewing the results of our OPSEC assessments, we learned that approximately 80 percent of OPSEC recommendations derives from OPSEC awareness among our people. Therefore, OPSEC awareness has been a high priority effort.

In 1991, we developed an unclassified, 12-minute OPSEC video titled "The OPSEC Picture Puzzle." The video, filmed on location in Las Vegas and at the Nevada Test Site (the site of the nation's underground nuclear weapons tests), provides an overview of the OPSEC program and how seemingly innocent activities of employees can become a piece of the OPSEC puzzle.

In order to increase awareness of OPSEC concerns, we developed an OPSEC cartoon character called Arnold OPSEC. The cartoon character is based on the adage that a picture is worth a thousand words.

The cartoon feature demonstrates various day-to day activities and identify the OPSEC concerns such as advertising vulnerabilities, what could happen when discussing sensitive information in public places or over unencrypted radio or cellular telephone communications systems, throwing sensitive information into the unclassified waste, or leaving sensitive information in an unlocked vehicle.

To date, we have developed 26 different features, with more on the drawing board.

An OPSEC poster was developed indicating that:

O perational
P procedures
S hould be
E Everyone's
C Concern

We developed a small "Pocket Guide to OPSEC" that defines basic OPSEC terms, describes intelligence collection methods and sources, answers the question "Why OPSEC?" and provides basic OPSEC measures.

As a part of my OPSEC program I utilize two symbols: one to portray a threat and the other to represent the attributes of a defender.

The first symbol is that of a purple dragon, taken from Operation Purple Dragon.

The second, representing that of the defender is, quite logically, a knight. Since we are all responsible for OPSEC, the knight represents each one of us as a defender of the OPSEC cause.

Additionally, not wanting to be outdone by military organizations that have their own distinctive motto, we have developed an OPSEC motto for the DOE Nevada Field Office: PROPUGNATOR CAUSAE or Defender of the Cause.

SUMMARY AND CLOSING COMMENTS

This brief article gives you an overview of the OPSEC program at the DOE Nevada Field Office, as well as some of our OPSEC awareness methods and techniques. Many of the methods and techniques are innovative and unique within our OPSEC community.

At the beginning I mentioned that methods and techniques have been modified and improved over the years by OPSEC professionals. A key element to the continuing development of OPSEC as a professional is the sharing of new methods and techniques. I hope that this article has provided you with ideas to further develop your OPSEC program.

In closing, I would like to say:

FIGHT FOR GOOD OPSEC BECAUSE SOMETIMES THE DRAGON WINS.

Kurt W. Haase is the OPSEC Program Manager for the U.S. Department of Energy in the Nevada Field Office, Las Vegas, Nevada.

OVERSIGHT: A Means to an End-- Not an End In Itself

Ethel R. Theis

Oversight of Government programs and activities deserves attention for a number of reasons. One reason is that, in today's world, oversight is ubiquitous. While oversight bodies have historically been a feature of government and private enterprise, their numbers have increased dramatically in the post-world War II years. All we have to do is look at our institutions to confirm that this is the case. Oversight bodies are found at every level of government and in private industry as well, although they are less prevalent there. It is no coincidence that the oversight function is considerably more prevalent in democratic societies. The voting public and its elected representatives expect accountability.

Oversight takes a wide variety of forms, both within government and in the private sector. Among the factors that influence the exercise of oversight are the assigned mission of the oversight body, leadership styles, perceptions of what constitutes oversight, and whether policy or operational oversight is involved. For example, an oversight body may choose to exert its influence rather loosely, devoting little time or attention to the programs or activities under its jurisdiction. This oversight body tends to show little concern for either the manner of program implementation or the achievement of program goals. At the other extreme, an overzealous oversight body might interpret its oversight responsibilities in such narrow terms that the autonomy of those charged with program implementation would be severely restricted. Clearly, neither of these approaches successfully promotes oversight objectives. Operating somewhere between these extremes, managers should seek to assure compliance while allowing those charged with implementation sufficient freedom of action to carry out their responsibilities.

This article discusses oversight of the Government information security classification program in the context of the experience of the Information Security Oversight Office (ISOO). It examines evolution of ISOO's approach to oversight, contrasting the early phase with its current approach and pointing out the benefits and drawbacks of each. ISOO's on-site inspections will illustrate the differences. Although somewhat sketchy, this examination of the two approaches should lead to conclusions as to which is more likely to enhance information security program effectiveness.

This discussion also indicates how ISOO would approach oversight of national industrial security policies. Clearly, the remarks concerning industrial security are speculative because the National Industrial Security Program (NISP) has not been formally launched. While the current draft of the executive order on industrial security assigns to ISOO the responsibility for policy oversight, coordination of the draft within the executive branch and industry continues. Until the process is completed, the identity of the policy oversight body cannot be stated with certainty.

On-site inspections are emphasized only because they are the activities most visible to security professionals, and the most reported. Their visibility encourages many security professionals to believe that they are the most significant of ISOO's activities and involve most of ISOO's time and resources. It may come as a surprise to many, however, to learn that this is not the case. In fact, several other activities take a comparable proportion of ISOO's time and resources, as shown in Figure 1.

"...managers should seek to assure compliance while allowing...freedom of action..."

KEY ISOO RESPONSIBILITIES

- Representing the Administration position on classification matters before Congressional committees, media representatives, and professional organizations.
- Responding to oral and written Congressional inquiries concerning specific aspects of classification policies and programs.
- Proposing changes to information security policies in response to changing conditions or perceived gaps in current requirements.
- Evaluating and taking action on complaints and suggestions from persons within or outside the Government with respect to the administration of the information security program.
- Developing broad guidelines for agency use on the scope and content of security education and self-inspection programs.
- Reporting to the President annually on the status of the classification system, and identifying areas in need of attention.

Figure 1.

THE EARLY YEARS: OVERSIGHT AS AN END IN ITSELF

Over the past decade, ISOO has discharged its responsibilities in two basically different ways. These were based upon contrasting styles of leadership and different perceptions as to what constitutes oversight.

ISOO initially approached this responsibility with a view that oversight is an end in itself. This approach influenced all ISOO activities, and perhaps none more than on-site inspections. In large measure, these were viewed as ISOO's primary and most important activity. And the emphasis was on quantity. Thus, the number of inspections conducted assumed more importance than their depth or quality. At times, the inspection program seemed to resemble a "bean-counting" exercise, in which a large number of inspections was equated with quality oversight. This approach did not require ISOO to distinguish between policy and operational oversight. Indeed, the approach encouraged a blurring of the distinction between the two.

The central characteristic of these early on-site inspections was an emphasis on compliance. They followed the ISOO checklist almost rigidly. As a result, the process became mechanical. During inspections, ISOO analysts were primarily responsible for obtaining responses from agency security officials to the checklist items. Formal inspection reports were provided to heads of agencies or senior officials for follow up. But they were primarily descriptive, often containing information already in the possession of the inspected agency. For example, the reports included detailed descriptions of agency security structures without analysis or even comment. Although such information helped ISOO gain an appreciation of the agency security organization, its inclusion in reports to agencies served no useful oversight purpose.

Contrary to what many may think, oversight as an end to itself, has a certain appeal to some people. It does not require a large staff, nor does it require much in the way of training personnel for oversight. For example, those conducting inspections need not be well versed in the nuances of classification policies and procedures. Rather, actions are fairly straightforward: the oversight manager develops a checklist, and the inspection team verifies compliance with the items on the list.

Another perceived benefit of such periodic inspections is that they discourage practices deviating from established policies and procedures.

Perhaps the major weakness of oversight as an end in itself is its amassing of detail, which causes everyone to lose sight of the larger picture.

Another significant weakness of the early philosophy is that it did not promote a harmonious working relationship between the overseers and the monitored. If anything, it fostered an antagonistic relationship.

For ISOO, the ultimate goal of classification oversight is to enhance overall program effectiveness. Therefore, over time ISOO has developed a perspective that considers on-site inspections as a means to an end. This was designed to overcome the failings of oversight as an end in itself, and to increase ISOO's contributions to overall program effectiveness.

THE PRESENT PHILOSOPHY: OVERSIGHT AS A MEANS TO AN END

General dissatisfaction among ISOO staff members with oversight as an end in itself, along with new leadership, brought about a change. Not everyone on the staff welcomed the change, and some were wedded to the old ways of doing business. For those resistant to change, the new approach can be intimidating. Nevertheless, as the ISOO inspection program evolved over the next few years, most of them functioned effectively under the principle that oversight is not an end in itself but a means to an end.

Perhaps the most important change brought about by the change in leadership and the new approach is the widespread recognition by the staff that ISOO deals with policy oversight, along with all that entails, rather than operational oversight. Figure 2 helps clarify the distinction between policy and operational oversight.

This recognition had an effect on the ISOO inspection process. The most striking change was a shift from a primarily descriptive to an analytic emphasis. Staff members were required to gain a new and broader understanding of the process. No longer would they view inspections solely from the standpoint of compliance with existing policies and requirements. Instead, during inspections, they collected data, evaluated it to determine the adequacy of classification policies and procedures, and, when appropriate, searched for the sources of weakness.

Rather than examining the requirements of the classification system in isolation, their analytic approach involved searching for causal relationships. For example, lack of familiarity on the part of classifiers with information security policies and requirements might result from a number of causes. Under such circumstances, the analyst must determine the sources of the problem:

- Lack of training
- Training not directed at needs of classifiers
- Low status of security function in the agency
- Lack of support from senior officials

CONTRASTING OVERSIGHT RESPONSIBILITIES

Policy Oversight

— Do program managers meet stated goals and objectives?

- Are goals being achieved?
- Where are the shortcomings?
- What can be done about them?

— Does policy require changes to improve performance?

Operational Oversight

— Do program managers follow the rules?

- Which resouces are committed to program implementation?
- How are operating procedures to be developed?
- Who is responsible for day-to-day operation of the program?

— Does conduct of the program require changes to conform with the rules?

Figure 2

Determining the causes and sources of particular problems is essential for meaningful recommendations for improvement. This action alone can contribute to a more effective classification system. On the other hand, if an inspection discloses an excellent program, determining the reasons for that success makes it possible to share those lessons with agencies that are not doing as well.

Identifying problem areas and resolving them in a timely manner are critical for individual agency programs, as well as for the Presidential program as a whole. It is not uncommon to find individual agency security staffs responsible not only for information security but also for industrial, personnel, and systems security. This limits the amount of time they can devote to in-depth internal inspections. In such cases, the findings of ISOO inspections become particularly useful as an impetus for improving the effectiveness of their programs.

An added advantage of this approach is that it fosters a cooperative relationship between the ISOO staff and that of the agencies being monitored. Both view their roles and responsibilities as complementary. The overall perception, and one that ISOO actively encourages, is that both are working toward a common goal: An effective and efficient classification system.

As agency programs are reviewed and problems identified and resolved, ISOO derives significant benefit from its position as overseer of the entire classification system. This vantage point allows ISOO to detect systemic shortcomings and to find ways to overcome or compensate for them.

Two weaknesses of the *oversight as a means to an end* approach deserve mention. One is that it requires a well-trained staff with analytic skills. Clearly, the analysis of data is significantly more complex than describing facts, and requires more care in its application. Simultaneously, management needs to make explicit how it expects the staff to conduct their analyses so that good analytical principles can be applied uniformly. Also, it requires that the staff be fully conversant with the nuances of classification policies, and the procedures that must be used in reaching informed conclusions and in making recommendations.

PROPOSED NATIONAL INDUSTRIAL SECURITY PROGRAM

Government and industry security officials have worked very hard for months to simplify the industrial security program and make it more effective. The current proposal is to establish and implement a NISP by means of an executive order. The draft order establishes policies and requirements for industrial security; it also assigns responsibilities for policy and operational oversight. The most recent draft makes ISOO responsible for policy oversight, with operational oversight vested in the Secretary of Defense (SECDEF) as the executive agent.

If ISOO were assigned policy oversight, its inspection program for industrial security would resemble its information security program. ISOO would conduct compliance visits at least once a year, and each would be conducted by one or more analysts. As to their scope, ISOO would review selected aspects of the program as opposed to covering all aspects of industrial security each time.

ISOO compliance reviews of the industrial security program would differ in one significant way from those for the information security program, however. Assuming that the Defense Investigative Service (DIS) exercises operational oversight for the SECDEF, the ISOO reviews of the NISP would concentrate on the DIS regions. ISOO would also review programs of the Central Intelligence Agency, the Department of Energy, and the Nuclear Regulatory Commission in specific areas. In addition, ISOO would visit a few area contractors during these visits. But it is well to stress that its primary concern would be with the manner in which Government agencies implement the NISP. ISOO would also produce formal written reports documenting its findings, and each report would be addressed to the agency head concerned.

CONCLUSION

Admittedly, this discussion of oversight philosophies and their impact on program effectiveness has been rather limited. It has concentrated on the experiences of one oversight entity: The Information Security Oversight Office. Nonetheless, ISOO's experience with two contrasting approaches to oversight offers lessons that might be generalized to other such bodies. What must be kept in mind is

that the purpose and character of the oversight entity will have a significant impact on program implementation. If its purpose is framed in narrow terms, the program under its responsibility may suffer. By contrast, a keen awareness of purpose and dedication to policy accomplishments will enable the oversight body to contribute to a more coherent and effective program.

Ethel R. Theis is Associate Director of the Information Security Oversight Office.

TITLES AND AUTHORS OF PREVIOUS *VIEWPOINTS* ARTICLES

NCMS *Journal*, Volume XXVI, 1990 [Published June 1991]

PART II - NCMS Viewpoints

TITLES AND AUTHORS OF PREVIOUS *VIEWPOINTS* ARTICLES

NCMS *Viewpoints*, Volume I, 1992 [Published February 1992]

NCMS Guidelines for Submitting Articles for Publication

- Submit four copies of each article.
- If possible, include a 5-1/4 inch floppy disk using WordPerfect software.
- Type with double-space and generous margins.
- White 8-1/2" by 11" paper must be used.
- Cover page should provide a title and any desired subtitles, but no personal identifying information about the author(s) to ensure objective consideration by the NCMS *Viewpoints* editorial review board.
- Forwarding letter(s) should be signed by the author(s) to indicate that all the required information is included and all material has been reviewed for accuracy and completeness.
- Signed forwarding letter should also bear this statement:

  "The material in this manuscript is the original work of the author(s) who forwarded it, except as noted herein. This manuscript has not appeared in, nor is it currently under consideration for publication in, any other periodical of general professional circulation. No classified information is contained in this manuscript. The author(s) certify(-ies) that he/she/they have complied with agency and/or corporate requirements for review and the manuscript is cleared for open publication. Further, the author(s) understand(s) that NCMS will copyright the published manuscript and will give permission to reprint it."

- Name(s), address(es), telephone number(s), and any other personal identifying information [*e.g.*, biography(-ies)] should be in the forwarding letter or on a separate sheet of paper, but not on the manuscript.
- Acceptable subject matter encompasses the broadest range of professional information appropriate to NCMS members.
- Commonly-accepted professional standards of propriety, civilized discourse, and discretion should be observed.
- No specific length is established, but authors should include both illustrations and aids to editorial reduction for particularly extended dissertations.
- Please note that NCMS will copyright the published article, but author(s) will be allowed to reprint without restriction.