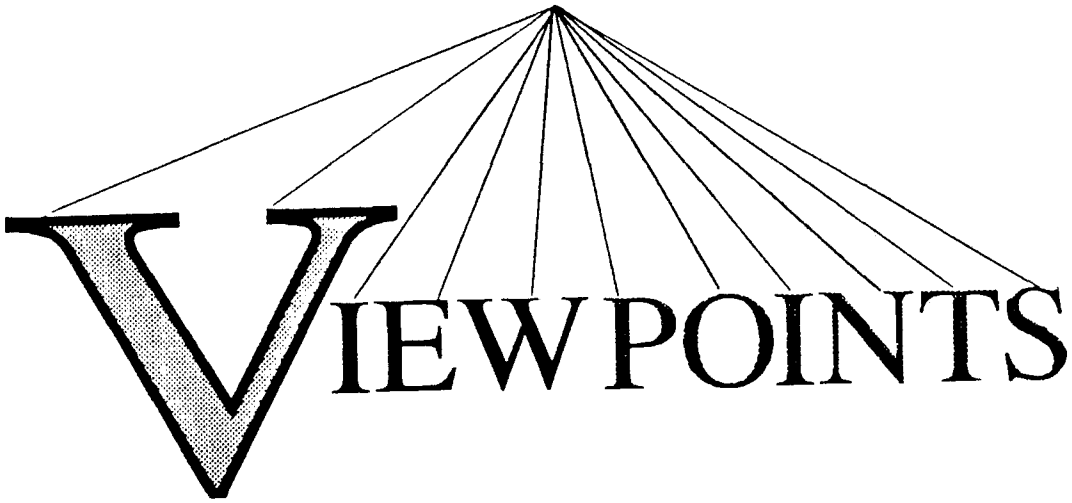
A PUBLICATION of the NATIONAL CLASSIFICATION MANAGEMENT SOCIETY
VOLUME 1, 1994

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 F. Donner, General Research Corporation; Marilyn H. Griffin, Naval Coastal Systems Center; James H. Mathena, Martin Marietta Corporation; Arvin S. Quist, Martin Marietta Energy Systems. 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.



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

The past year may have been a watershed for classification management in the United States. It will probably be some time before we know clearly the full consequences of all decisions made or still pending. Nevertheless, National Classification Management Society (NCMS) members deserve to be kept informed of activities that affect, or may affect, their professional lives.

In keeping with article II of the Bylaws, Viewpoints provides one of several NCMS forums for the free exchange and dissemination of information and views on matters of interest. Regrettably, no one in (or outside) the Society has yet announced possession of a crystal ball to discern the effects of ongoing and proposed policy initiatives. If a Viewpoints reader should happen to be clairvoyant, however, please accept this invitation to enlighten our membership in the next edition. In the meantime, readers are invited to read the views printed in this issue of several informed authors regarding proposed changes to the US information security program.

In Presidential Review Directive (PRD) 29 of 26 April 1993, National Security Advisor Anthony Lake established an inter-agency task force and charged it with producing a revised executive order for national security information by the end of last year. In June 1993, Director of Central Intelligence James Woolsey and then-Secretary of Defense Les Aspin created the Joint Security Commission (JSC) to devise ways of coping with mutual security problems of these two agencies. And, once President George Bush signed the National Industrial Security Program (NISP) executive order in January 1993, the NISP Steering Committee began coordinating drafts of an Operating Manual for publication within the time limits set by Executive Order 12829.

Any one of these three initiatives would have challenged Government and industry security specialists. In their totality, they present an enormously complex maze of issues and concerns that might easily overwhelm officials (or NCMS members) who have professional responsibilities for classifying, safeguarding and declassifying national security information.

Several experienced authors have stepped forward to offer NCMS their experience, insights, and judgments on issues raised by these initiatives. Readers will appreciate that the authors featured in this edition of Viewpoints expressed these opinions at the end of 1993, and did not have the advantage of reviewing the most recent output of the task force, the JSC or the NISP Steering Committee. In a sense, however, their comments are timeless because the issues involved appear to have no final solutions that are universally applicable. In another sense, readers may find their contributions timely if this country now chooses to hold a public discussion or debate about the issues, the facts, the problems, the viability of proposed alternative solutions, their costs to the taxpayer, and their effect on and implications for our national security.

Maynard C. Anderson responded affirmatively to an invitation for writing a guest editorial as his parting words to NCMS members. His article is adapted from several speeches he delivered in late 1993, with additional observations on visible policy review activity up to his retirement in early February 1994. Drawing upon more than 36 years of Government service, he gives both pros and cons of our past and current efforts to reform the information security program. Please read his entire article before you formulate your final opinions. Otherwise, you may reach an incomplete or incorrect conclusion about his answer to the rhetorical question, "Is the future behind us?"

Gerald L. Kovacich presented his article on the NISP for publication last summer. It remains valid today, although some organizational changes are appearing on the horizon. Certainly his urging that Government

and industry work toward achieving standardization and better cooperation expresses long-standing sentiments of many professional security specialists.

These two articles demonstrate that numerous issues surrounding national security information policy are contentious. They have given rise to widely divergent viewpoints even among Government and industry security policy theoreticians and program practitioners. Outside these circles, the fourth estate has given a national forum to criticisms by special interest groups and others who are dissatisfied with that policy. Some of the critical views expressed are based upon personal or relatively narrow experience, while others obviously can be attributed to perceived or real unsatisfactory treatment. In any event, no one should doubt the sincerity or convictions of these members of the American public. In this regard, citizens and officials alike often face the same frustrations with policy and resource limitations of the information security program as they might on tax matters, court proceedings, veterans issues, law enforcement, health care, or estate property settlement actions. In short, with all public policy.

But information security policy attracts particularly highly charged views because of our democratic heritage. The US news media are often expected to present the citizens' concerns to Government, sometimes giving little space or time to a reply, an explanation, or justification. Perhaps this imbalance is calculated to redress a perceived powerlessness of certain special interest groups to help shape national security policy. Indeed, some groups may object to being denied access to classified information upon their demand because they suspect that national security is not the real reason for withholding it. Generalizing about the variety of circumstances is simply not possible, however; each case should be evaluated on its own merits and conclusions withheld until all the facts are known.

Speculating about the reasons for these divergent views still leaves us with the question about how to improve our security programs and to achieve greater openness without destroying the effectiveness of programs designed to protect our national interests. For a fresh perspective, we turned to an "outsider."

David B. Fell, Jr. is not a security specialist but an engineer with extensive security experience who put his thoughts in writing during the summer of 1993 to help Government officials evaluate alternative proposals to current national security policy. His perspective deserves the attention of defenders and critics alike. This may be one of the few articles in print that provides a coherent argument presenting the what, the why, and the how of security protection in clear language. It could serve as a point of departure if we ever engage in informed public dialogue about our information security program. If we mean to have a discussion, let it begin here!

Such a discussion might be further enlightened by reviewing some of the articles published in previous issues of Viewpoints. For convenience, the titles and authors are listed in the back of this edition. Once again, your submissions will be easier for the editorial review board to consider if they meet the NCMS requirements stated on the last page of this edition.

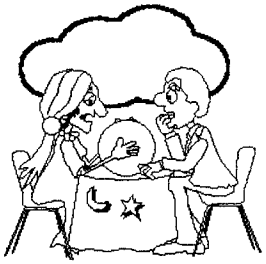
Our final contributor, Charles C. Wilson, discusses a new subject for Viewpoints. His article, "Security Policy for International Programs," began as a briefing several years ago, and gradually evolved into this abbreviated introduction to US programs for disclosing classified information to other nations. Preliminary responses indicate that NCMS members want and welcome a better understanding of international security programs. In this regard, the DoD Security Institute will offer a week-long course on this subject to Government officials beginning with FY1995. If readers find Mr. Wilson's

article helpful, please let us know so we can arrange for related follow-on items of use to you.

Please note the editorial review board members identified on the reverse of the cover page. They read every proposed article and offer many valuable suggestions that help maintain the quality of Viewpoints.

A final note to explain the long delay in publication of this Viewpoints issue: Several large articles had been promised last summer. When they were not forthcoming in October as expected, we negotiated with authors on a new set of subjects. Thanks to exceptionally fast work by the Viewpoints editorial review board, all were approved by the new year. The flurry of official work relating to the revised executive order, JSC Report, and the NISP combined with the most disabling Washington winter in three decades to postpone printing until May 1994.

Guest Editorial



INFORMATION SECURITY PROGRAM:

Is the Future Behind Us?

Maynard C. Anderson

We are witnesses to a remarkable phenomenon in the world of information security today because, while almost everyone having something to do with the government's control of information is advocating change--even "radical" change, not much change is actually taking place. Certainly, the proposed information security changes offered for official review have been less than radical.

It should come as no surprise, perhaps, that proposed changes to the information security system are not remarkable. Government policies concerning information security promulgated through a series of executive orders (EOs), beginning with EO 10290 issued by President Truman in 1951, have evolved, with minor reasonable aberrations, from imposition of firm control over nearly any information that anyone wanted to protect, to imposition of firm control over almost all information that almost everybody wants to protect. Successive information security executive orders, generally, have made minor changes to archaic policies that were applied randomly, inconsistently, and intermittently. Today, there is a widely accepted conclusion that the information security program is inefficient and there seems to be no one in charge overall.

"Today, there is a widely accepted conclusion that the information security program is inefficient, and there seems to be no one in charge overall."

There has always been great difficulty in devising classification standards that clearly identified the information that really needs protection. Without such standards, classification authorities continue to decide that information needs protection without providing adequate justification. Steven Garfinkel, Director, Information Security Oversight Office (ISOO), has said that "If somebody asked me what we will be keeping secret in the future, I would say the same information. There is less of it, but the same information."

Unfortunately, Mr. Garfinkel is probably right in his assessment of the kinds of information that will still be subject to protection; whether there will be less of it is arguable.

Overclassification, incorrect classification, and classification in ignorance have all contributed to the massive amount of information currently protected. Other contributing factors include the absence of challenges to improper classification, assignment of unreasonable durations of classification, and failure to allow declassification except by individual document review. Perhaps the proximate cause for the general failure of the information security program to function effectively in fulfilling its principal dual missions of protecting and disseminating information is the absence of someone in charge to enforce current rules while devising new, modern policies and procedures.

Another contributing cause to maintenance of the status quo, certainly, and one that mitigates against radical change, is that most government personnel who administer the information security program are risk averse. They do not like change because it makes them

uncomfortable, it makes them work harder, and it threatens their employment when it results in efficiency and reduces personnel requirements. Further, they have been trained in a discipline that rewards them for operating within strict boundaries and sets of rules. Their rationale for maintaining those rules is logical: the national security would be in jeopardy if the rules aren't followed; a classification authority has made a judgment by electing to protect the information in their custody, and if they fail, they and the nation might suffer. Better be safe than sorry.

"A new classification system will not come from within."

It is impossible not to agree with Steven Aftergood: [1] "A new classification system will not come from within. Mounting financial costs will force some incremental changes, and periodic controversies like that surrounding the Kennedy assassination will compel greater openness in highly specific areas, but more systematic change will not come voluntarily. As one State Department official put it, "No one is going to streamline himself out of a job'."

These comments should not be construed as critical of the dedication and devotion of most information custodians in our government. They are well-intentioned, and some of them would contribute to improvement if given the chance. That notwithstanding, individual actions make the systems and the institutions work, so we must all accept part of the blame when things don't work so well.

Except for a few periods of optimism on my part when I thought that we would rise above the continuing cycles of bureaucracy reinvention, I must conclude that mediocrity has reigned in the administration of the United States information security program. Our failures have not been fully manifest in the compromises of classified information, in the leaks, or in the espionage cases that demanded publicity. There have been few of those. Our deficiencies are clearly evident in failures to show our leadership the rightful place of security in the management of our organizations; in our failures to identify and implement a concept of security that protected only what is essential; and in our failures to articulate a philosophy of security that, per se, proved its necessity.

The National Industrial Security Program (NISP) is a good example of the many difficulties involved in bringing even a highly publicized and desirable proposal to fruition. The NISP was conceived as a means to standardize policies and procedures for security in industry. The proposed new program would have been more efficient and more economical, and would have provided better security. It was envisioned as a precursor to standardized security policies for the government in general.

The initial concept included development of a Presidential policy document that would have combined the provisions of EO 12356 with those of EO 10865 that pertain to information protection. That concept made sense because "industrial security" is nothing more than the protection of classified information the government loans to industry for performance on contracts. As a part of the information security program, therefore, it should derive its authority from the executive order concerning protection of national security information.

"The national security community found itself in the peculiar situation of having what many believe is a seriously flawed executive order directing implementation of a NISP before the reissuance of the basic information security executive order from which industrial security provisions are, in fact, derived. A cart-before-the-horse situation seems to have been created."

Unfortunately, as the "mating dance" between EO 12356 and EO 10865 was underway, officials of the Department of

Defense, fearful of possible adverse Congressional reaction, dissolved any prospects for the union. They mistakenly attributed the furor in Congress over some of the provisions of NSDD-84 [2] to the debate over the information security executive order. Consequently, the DoD officials pursued separate authority for the NISP. As a result, EO 12829 was conceived and issued by the President as a separate charter. The national security community found itself in the peculiar situation of having what many believe is a seriously flawed executive order directing implementation of a NISP before the reissuance of the basic information security executive order from which industrial security provisions are, in fact, derived. A cart-before-the-horse situation seems to have been created. And, now, implementation of the provisions of the NISP executive order has been delayed pending results of a Joint Security Commission, the Charter of which pertains to the DoD and the Central Intelligence Agency (CIA) only. The cart-before-horse situation has thus been further complicated by an enigmatic anomaly, wherein not all affected agencies are working through the policy issues. How can we expect uniform implementation?

Historically, efforts with which I am familiar to modify each successive executive order and to establish information security policies that meet modern needs have been unsuccessful. These policies have not kept pace with international developments, technology advances that involve different media for transmission and storage of information, or the need for a program that integrates information protection with personnel security on a national level.

Lest the reader feel that there have not been any program accomplishments, we should recognize that there is an increasing awareness among all personnel concerned with information security of the need for policy and procedures improvement. Also, there is an increased recognition within the DoD that supplemental protection of information through the indiscriminate use of special access programs isn't as necessary as was once believed, nor is it worth the cost.

Professionalism of our personnel has improved. The creation of the DoD Security Institute (DoDSI), the Defense Personnel Security Research Center (PERSEREC), and the DoD Polygraph Institute (DoDPI), for example, have made available means by which people can and are expected to improve their professional capabilities. Coordination of international policies concerning industrial security, through creation of the US-led Multinational Industrial Security Working Group (MISWG), has eased some of the burdens of United States industrial firms operating in Western Europe. The Defense Investigative Service (DIS) continues to modernize and improve its service to industrial firms engaged in classified contracting. The Security Policy Automation Directorate (SPAD) in the office of the Under Secretary of Defense for Policy has improved the Foreign Disclosure and Technical Information System, implemented the Foreign Visits System and the US Visits System, all of which improve the opportunities to ensure the secure disclosure of US classified information.

"Risk management has been practiced in the Defense information security program almost since its inception."

Risk management has been practiced in the Defense information security program almost since its inception. A notable example was the decontrol of secret information in the DoD in 1978, which was an accomplishment of significance that increased the timely dissemination of information to those who needed it. Elimination of the need to specifically account for each classified document within a facility also saved great amounts of time and resources, particularly for those organizations processing large volumes of information.

The requirement to develop and promulgate security classification guides was an accomplishment that diminished the amount of classified information and material that originated in the department. The need for security classification guides causes the program managers to begin thinking about information protection at the earliest stages of program planning. The guides, along with mandatory portion marking, another accomplishment, have been systematic, effective, and efficient means to specify various levels of protection within programs.

The Acquisition System Protection Program has now been initiated in an effort to ensure that security is considered at the outset of acquisition planning in the DoD.

The information security program of the Department of Defense is the best understood of our security programs because its requirements reach to the lowest level of every organizational element that handles classified information. As a result, it has been a conduit for improvement in other related security programs, like security awareness and the continuing evaluation of cleared and accessed personnel.

* * * * *

What lies ahead? What needs to be done? What should be our focus? What can we do to escape from the war-time model (WWII, not the Cold War) of information security that has been our guide? I will try to explain how I view current circumstances and prospects for the future so officials can work out answers to these questions.

Information became the real treasure of the twentieth century. It is reported that the information available to us doubles every five years. It will quite likely be considered the critical commodity of the twenty-first century. It should be treated with the respect it has earned and the value it will probably assume. That treatment must include not only protecting and preserving the information that has value to our national security at the moment, but disseminating and using information in ways that are beneficial to our national interest in terms of political relations, economic advantages, and military relationships.

I anticipate that classification management will be recognized as a principal solution by more and more government officials; that information custodians will take more realistic approaches to the release of information from the constraints of protection; that a truly comprehensive program of information management will be accepted by the federal government and that it will include protection of classified and unclassified information; that a rational theory of security will emerge in which personnel security and information safeguarding will be integrated as policy principles; that the proper balance among statutory opportunities for both protecting and releasing information will be recognized in the formulation of national policies.

Concerning classification of information, the challenge of "Why?" will emanate more often from more challengers as the concept of open source exploitation of information in environments like those of coalition warfare, peacekeeping, and humanitarian assistance take more of the resources of our military forces. Imagery obtained by technical means from overhead sources is becoming a commercial commodity no longer subject to wholesale embargo. In counterpoint, while some of the more rigid and intense protective measures may disappear, new and different countermeasures will be needed to protect even unclassified "sensitive" technology and information being manipulated by multi-media, complex communications, and incredibly capable dissemination systems.

"There are legitimate reasons for protecting information: to preserve human life directly or indirectly; to protect operations; and to protect intelligence sources and methods and advanced systems and countermeasures. There are few other justifications for imposition of severe constraints on information distribution."

Information classification levels are arbitrary, artificial designations of information sensitivity devised by program managers often to satisfy desires for exclusivity. There are

legitimate reasons for protecting information: to preserve human life, directly or indirectly; to protect operations; and to protect intelligence sources and methods and advanced systems and countermeasures. There are few other justifications for imposition of severe constraints on information distribution.

In the future, I believe that official information should be born unclassified unless conclusive proof is offered that it must be protected. The proof must rely on the information's value to the national interest. The development of dual-use technology that has been directed by President Clinton requires that information may be classified only when that technology is of such value that, when applied in support of the national security, the national interest would sustain irreparable damage through its compromise. And, classification should be allowed only if other already existing statutory means of protection are insufficient.

We will be forced to determine all security requirements on an entrepreneurial basis because of improving methods of development and more sources of foreign availability of technologies once judged as critical, along with an increased need to maintain US industry's competitiveness through sharing of defense information, technologies, and weapons with allies, friends, and former foes. Are we far enough ahead of our competition to forego protection through classification?

Special access controls will not be affordable except when the protection of the highest level of classification is insufficient. That is the standard now, but it hasn't been followed.

We must identify technologies and technological solutions along with better management techniques to protect information in its two most vulnerable environments--automated systems and the human memory. Computer terrorism that results in the theft or manipulation of information in systems, sometimes for economic gain, must be anticipated.

Less and less of our classified information will be in tangible form like paper documents. More and more will be in automated information systems. The extraordinary physical protections given to paper products will no longer be necessary. The different perils of transmission and storage in automated systems will require different treatments.

Only those physical security measures will be allowed that match the value of the information with the vulnerabilities and threats of the environment in which it is used or held.

There is no easy answer as to how we will control our information that needs protection, but there is a high probability that selection of the best and most efficient countermeasures to protect our national interests in the world's new circumstances will probably cost more money. Another significant future challenge will be to match the value of the information with the costs of its protection so that we achieve the greatest benefit.

In the modern world, it should be recognized that "value" is the quality which, when assigned to information, defines the information's worth in terms of its usefulness or importance to the national interest. Such a definition should be included in an executive order along with "value" as a basis for classification.

Use of "damage" as the principal test for the validity of classification of information is insufficient because the extent of our adversaries' holdings of the information is unknown (if they already have the information, there is no damage and without knowing what they have, a damage judgment cannot be made); possession of the information by an adversary who does not choose to use it or may not be able to use it causes no damage; and prediction of damage is postulation about a future condition, which is difficult even under the best circumstances.

Additionally, protection of information that is vital to the national interest may be required whether or not its disclosure causes damage. Information might be of value because it saves lives or resources, or provides a known technical advantage or is known to be wanted or needed by adversaries. The judgment of something's value is based on factors that we

can identify now and over which we can exercise effective control or management. A positive current example might be the one in which the value of information that enables the United States to successfully compete in the global economic market place may well require the information's protection, even though possible damage resulting from a failure to protect the information might be impossible to identify. The identification of information's value by a classification authority would be positive, tangible, and comprehensible to any reviewer of the process. In combination with the element of damage, the use of value as a criterion would diminish the amount of classified information by eliminating protection of that which is speculative concerning possible damage caused, that which is frivolously designated without justification, or that which is classified to protect the sins of the classifier rather than the national interest.

In the spirit of reinvention, a category of information eligible for classification if its disclosure would adversely affect the economic security of the United States should be in an executive order. Adding a category of economic security recognizes the evolving importance of the competitive position of the United States in the world market place. It justifies the necessity of protecting the military application of dual-use technology while that same technology might be exported to a foreign national as a component of a civilian product. It emphasizes the principle of classification in accordance with information's value to the national interest and is in accord with the creation of the National Economic Council.

The President should recognize the integral relationship between information security and personnel security by including in a new order the provision that personnel may be granted access to classified information if that person has met the requirements for a security clearance as outlined in EO 10450 or its successors. It seems incongruous to issue an executive order specifying all of the provisions for control and safeguarding of information while dismissing personnel security by omission. Information is principally dependent on the people to whom access is granted for its protection, and requiring a personnel security standard will improve the ability of agency heads to manage the dissemination of classified information.

A number of specific suggestions for future improvements must deal with special access programs. The suggestions are based on the premise, applicable to all information, that the only way to reduce the amount of classified information is to treat the proximate cause by establishing higher standards for classification or compartmentation--in other words, deal with the problem up front.

The proposed order to replace EO 12356, for example, establishes the special access program standard as one in which the vulnerability or threat to specific information is exceptional. I would propose, rather, that information deserves special protection if it is of such sensitivity that its value to the national security is exceptional, and its value to actual or potential adversaries is exceptional, based on evaluations of their current knowledge, intentions, and capabilities in contrast to US capabilities and strategies. The reason for that is that threats and vulnerabilities are important as factors in program management's attempts to determine what protection techniques to apply. They are not, per se, acceptable reasons for the creation of special access programs. The only reason to create a special access program is to protect information that is of extreme sensitivity to the national security of the United States.

It must be emphasized that creation of a special access program should not be allowed before the protections afforded by the highest level of classification available have been exhausted. Upgrade criteria from the baseline classification program must include a presumption that this information security program cannot provide the necessary protection because of the sensitivity of the information. Therefore, information protected by a special access program must be classified at the highest level before application of supplemental controls is allowed. Such restriction will diminish creation of programs using compartmented protection and will ensure that supplemental protection is used only in those programs that control information of extraordinary sensitivity.

These recommended changes are based

on the fact that there is always contradiction between protection and dissemination of information. That conflict, along with the world changes that we recognize, demand that we agree on new definitions of information, material, and system sensitivities in the context of modern technology and political dynamics rather than on the basis of outdated philosophies and requirements. We need to develop and implement a concept of security that is not category dependent, but that includes the integration of every discipline and every means to properly manage the control and dissemination of things of value.

While not the most enthusiastic supporter of total quality management (TQM), I believe that application of some of its principles and techniques to the information security program might be beneficial. There are no reasonably effective means employed to determine whether, if, or when the program is effective. There is no effort to determine quality on which to base improvement, when required. And, most importantly, perhaps, customer and client feedback analysis is seldom undertaken, or if undertaken, application of the results is seldom evident. This was vividly demonstrated during the PRD-29 [3] process when committees were established within the task force only to have their respective products ignored or disregarded by higher levels of the review hierarchy.

The people who must run the system, therefore, are not being allowed to participate in designing the system. Reviews of the information security program of the federal government, conducted prior to the formulation of each executive order that has been issued, have begun with the intention and, to some extent, the contributions of workers in the field. Unfortunately, their contributions are most often run through filters in the bureaucracy or ignored completely while an order is drafted and approved by officials who have no hands-on experience in administering or managing the program. In the current case, agency positions have been ignored while others lacking basic knowledge of program requirements, legal requirements, and administrative requirements have told us what is good for us once again.

Policy making is the translation of information into action. Generally, the best information concerning our process is with those who must implement the policy. The information security program is dynamic. It will be more dynamic as changes take place with greater speed and developing technology out paces policy.

More important, perhaps, is the fact that the information security culture is more than 50 years old. It will not change unless its constituencies cooperate and make it change. Directed actions derived from the work of non-professionals who ignore the culture will be ignored, in turn.

Automated systems are causing evolutions in both sensitivity and utility of information in terms of hours and minutes, not months or years. Establishing classification durations of 40 years is beyond the pale in most ordinary situations, and is an example of flawed policy now being recommended.

Aside from the difficulty in deciding what should be classified, the information security issues that capture most attention from management and executive personnel are classification, duration, downgrading, and declassification; probably because they are the aspects of information security that are most visible. The classification actions fuel the engine that drives personnel security, safeguarding, and accountability. Classification duration consumes resources for physical protection. Reviews for downgrading and declassification of the body of presently classified information would ensure that all available human resources would be occupied for many years if we were to pursue the process on the basis of present and proposed procedures. None of our experiments with systems of declassification have worked well.

We are frustrated in our attempts to determine the standards for initial classification or protection of information. Requiring protection authorities to rationalize the value of information in basic national security (includes economic security) categories would be a beginning. Authorities must be required to issue security protection instructions like classification guides for their programs, projects, or systems. The costs of overclassification must be avoided

in terms of unnecessary personnel security requirements for those needing access. The personnel security requirements established by the information protection authority document must be universally accepted. Individual department and agency requirements for personnel integrity for reasons other than security, such as for those personnel with fiduciary responsibilities, must be met by those department and agency assets. Similarly, myriad safeguarding and accountability processes must become unacceptable so that reciprocity among all departments and agencies will become the norm. Recent debate and discussion over how to achieve reciprocity in facility sharing has highlighted how the information security system has become degraded by the growing bureaucracy in some ways. A few weeks ago, I commented to Dick Sampson, Security Director of GDE, that we had the reciprocity problem solved thirty years ago when the principal agencies agreed to share each other's facilities. Dick replied that was true because then we just shook hands and that sealed the agreement. We need to return to the handshakes.

Automatic downgrading of information should be directed if, on balance, security resources would be conserved by lowering the classification from Top Secret to Secret, for example. If it is decided that a one level classification system is sufficient, declassification rather than downgrading would be the only option, of course. Information must be downgraded or declassified as soon as possible, but not later than twenty years from the date of classification. While agencies will ordinarily coordinate their reviews of national security protected information with other agencies, foreign governments, or international organizations that have direct interest in the matter, they should, in every possible circumstance, initiate action to declassify information of the same generic type or category, en masse, or in blocks without specific review of each media item (document, disk, etc.) on which information might be inscribed or recorded.

As presently constituted, the Information Security Oversight Office would work against great odds to enforce classification management of this kind throughout the government. An organization must be established with a charter to make rules and enforce them in the form of one national policy concerning the protection of valuable national information assets. Then the fragmented policy-making and enforcement could be prevented and resources allocated where they are needed most.

It is particularly important to formulate a national policy now because of our growing multinational security cooperation efforts. A national policy concerning information management and control would improve security, and simplify our cooperative agreements with allies and friendly countries by ensuring that we all play by the same rules. It would benefit the competitive position of American industry in the world market by standardizing information control requirements.

The President should designate an executive agent for information security who would assume responsibility for all aspects of information control and management through an information assets protection program. A standard system will work. We can no longer afford the diversity of the past in which information of the same sensitivity is provided different degrees of protection by different organizations. Traditional approaches have attempted to solve discrete problems. Declassifying large volumes of information without exercising strong management over the classification or control of new information will not solve the problem. A total systems approach that includes centralized authority and decentralized management will provide the necessary control as well as allow the exercise of creativity and innovation on the part of the system administrators to make the system work.

I have begun to define security of information, its control, management, and dissemination, in the context of the program's failures, proposals for program changes, and expectations of program improvements. We need to continue to perfect the definition in the context of the tension between defense security interests and economic security interests. Until we arrive at that definition, there will be inconsistencies in the way we apply the security provisions. In the end, we must reach that

comprehensive definition of security that includes economic, political, and military dimensions so the United States can join the future international competition while protecting that information which has legitimate value and using all of our technology to the Nation's best advantage.

Maynard C. Anderson retired in February 1994 as Assistant Deputy Under Secretary of Defense for Security Policy.

Footnotes

1. "The Perils of Government Secrecy," Issues in Science and Technology, Summer 1992, P. 81

2. NSDD-84, "Safeguarding National Security Information," was issued on 11 march 1983, by President Reagan with the stated purpose of reminding federal employees of their personal responsibilities in protecting classified information. It specified a number of additional steps to be taken to protect against unlawful disclosures of classified information. Among them were the development of two new nondisclosure agreements for government-wide use, one for classified information and one for access to sensitive compartmented information (SCI) that included a provision for prepublication review; policies governing contact between media representatives and agency personnel to reduce the opportunity for negligent or deliberate disclosures of classified information; new measures to investigate unauthorized disclosures of classified information to include the use of polygraph examinations under certain conditions; and a study of the personnel security program of the federal government.

3. Presidential review Directive 29 was issued by the President in April 1993 with the objective of reviewing EO 12356 and proposing policy for an improved information security program, with a due date of 30 November 1993.

An Engineer Looks At National Security Policy

David B. Fell, Jr.

An Assessment of Our Current Situation

The premise underlying recent criticisms of Executive Order 12356 appears to be that, with the end of the Cold War and the dismemberment of the Soviet Union, the United States should and can significantly relax its protective measures for classified [national security] information. Critics also advocate eliminating or reducing many of the national security organizations to streamline the Government and to reduce costs.

Unquestionably, the Cold War threats that we faced for some 45 years no longer exist in the same form or to the same degree. The US Government should recognize the new order of world power and redefine US national security to reflect that reality. Clearly, communist and socialist governments in eastern Europe and Asia failed convincingly. Furthermore, the Red Army's military domination of Europe has ended. And, as most observers will agree, the once-huge, heavily funded Soviet intelligence-gathering apparatus has been substantially reduced.

On the other hand, many other international and internal threats to our national security have surfaced, some in a dramatic and violent manner. In the post-Cold War era, these threats range from traditional antagonist nations through terrorist groups, and even include some current allies; both foreign government agencies and foreign industrial firms are represented. It is significant that counterintelligence agencies continue to catch traitors and to capture spies. Therefore, US Government and contractor security specialists are being advised to remain on the alert so they can thwart attempts by agents of foreign entities to obtain critical technology and other vital secrets.

Note, for example, that the number of countries and industries seeking advanced technologies has increased during the past several years. Many of them already possess modern technology and weapons manufactured by the US, our Allies, and the former Soviet Union. Some have access to most of the same intelligence collection and processing technologies used by military and state agencies of the USSR. Although such assets may no longer be available for employment on a large scale, foreign user organizations can now afford to focus on fewer but highly lucrative US targets.

During the years after 1985, the US defense establishment began to shrink, significantly reducing the number and diversity of targets that foreign interests needed to exploit. This process continues today, accelerated by military downsizing, base closures, facility and contractor consolidation, and initiatives that result in more joint and common programs. Therefore, the range of potential US military targets for hostile intelligence to exploit will remain smaller for the foreseeable future.

Concurrently, the pace of deploying new weapons systems has slowed. Today, our planning for the future envisions upgrades and life-extensions for many of our weapons systems rather than production and deployment of entirely new ones. We may continue, to some degree, to develop advanced concepts and even to conduct engineering development for some systems. But these, for the most part, appear to be headed for the shelf.

This means that our operational weapons and new technologies are being exposed to potentially hostile exploitation for longer periods of time because acquisition program review

periods and development cycles are strung out. Extending the time from conception of a new technology until it reaches full operational capability in a weapon or other system makes us more vulnerable to espionage and the consequences thereof. We can no longer escape the real-world consequences of classified technology losses and compromises, leaving them in the dust created by accelerated development of new weapons systems.

With smaller forces and longer-lived weapons systems, the need for security of our remaining assets increases. We will be dependent upon fewer weapons systems for longer periods of time. If classified systems are compromised, essential technological and tactical advantages may be lost when our forces face critical life-and-death situations. Recent experiences in trouble spots around the world demonstrate the value of tactical success to maintain support for US policies. Public opinion appears to become quickly intolerant of personnel losses and any perceived tactical deficiencies.

Finally, restructuring and refinancing of large corporations, increasing dependence on foreign sources and joint international manufacturing programs, and the increased use of shared automated data bases and communications networks dramatically increases the vulnerability of US industry to foreign ownership, control, influence, and espionage. Major domestic companies increasingly lose their US identities and become international in composition and ownership. With increased emphasis on acquiring commercial, off-the-shelf equipment, the distinctions between secure defense and open non-defense information risk becoming blurred. With large elements of the defense work force being terminated, numerous cases of personal financial hardship arise, creating disillusionment and, in some cases, bitter resentment. These create fertile conditions for security compromise, sabotage, and espionage.

The bottom line is that, **notwithstanding the demise of the Soviet Union, the real threat to national security information may actually have increased!** We probably need to increase our security. In any case, there is no reliable, statistically-valid quantitative assessment of the effectiveness or ineffectiveness of the existing national security program in safeguarding classified national treasures. Certainly we have noted failures and shortcomings under Executive Order 12356, but senior managers and executives must ask whether these reflect inadequate policy or inadequate compliance with policy that is basically sound!

My Approach to the Problem

Amid the pressures and frustrations of defense downsizing, it is easy enough to embrace broad criticisms of the existing system for safeguarding national security information, and to propose drastic cuts in the associated infrastructure. As a practitioner and observer of security measures issued by seven Presidents over four decades, however, I suggest that the present regulations do protect classified information. The chief problem, I believe, is they have become so burdensome that workers have lost sight of their value and find them onerous to implement; furthermore, security specialists cannot always effectively enforce them. Rather than making wholesale changes to or completely overhauling the security machinery, however, we should identify specific problems and concentrate on fixing these while reducing the quantity of information processed.

My approach to improving security regulations and the national security program consists of three parts: clarifying the vision; reestablishing rank-and-file support; and reducing the amount of classified information handled to manageable proportions.

First, we must publish a concise statement of goals, guidelines, and priorities clearly defining the vision from which all regulations and procedures derive. Then we should establish a program of total quality management education and motivation that

actively enlists workers at all levels in the protection of classified information. This would be accomplished not by slogans and posters, but through interaction and mutual support of program managers, security specialists, practitioners, and outside oversight persons. In parallel with this practical "security education program," we must significantly reduce the amount of classified information processed, and then control and limit access to that which remains classified.

What follows is a brief explanation of how we can effectively reduce and control the amount of information needing protection.

A Systematic Approach to Classification Review

Proposals regarding security classification reviews can be addressed under three basic scenarios: programs that are new; programs that are ongoing; and programs that are essentially complete (i.e., obsolete data).

The review procedure is essentially the same in each scenario. It involves program technical and management personnel working in conjunction with security personnel. Its purpose is to restrict the amount of new classified information required to be processed and controlled. Targeted savings and reductions should be substantial, say 75%. Reductions of such magnitude have already been realized by the Department of Defense in formal program oversight data: Government and industry, working together, refined the controlling parameters and characteristics by which program acquisition is authorized and measured using the Acquisition Program Baseline Agreement (APBA) process.

Moreover, security classification management should be formally tied to the acquisition review process, linking classified information identification and review to the APBA cycle. Essentially, an APBA is now required for each acquisition program, and must be updated at every milestone or program change. These would be good times to conduct classification reviews. For non-acquisition demonstrations, reviews would occur at program inception, completion, and any change of status.

Goals, Guidelines, and Priorities

The current Executive Order identifies nine generic types of information that may be classified, and provides for three levels of classification that are directly related to the degree of safeguarding required. Additional guidelines and precise classification criteria might help derivative classifiers more uniformly apply the decisions made and distributed by original classification authorities (OCAs).

At the outset, technical personnel should analyze the information elements of weapon systems and other programs to specify what information and data requires security protection. Program managers would then use the criteria to justify to the OCA why that critical information requires classification. The result should be an agreement to limit or reduce the amount of classified material by a reasonable amount.

Once technical experts and program managers have completed their work, OCAs would issue security classification guides, specifying precisely what information is classified. These guides should also be reviewed at each subsequent milestone. At those times the same review team would evaluate the critical APBA system data mentioned above, as well as critical new component and subsystem design disclosure, critical subsystem performance specifications, and critical manufacturing processes. In many cases, as weapons move toward field testing, other items will require security protection, such as tactical operational details, algorithms, and automated weapons processes.

Intelligence information must be protected, of course, including methods and sources. But every effort should be made to standardize and reduce the classified information needed in weapons systems development regarding threat characteristics.

In addition, increased emphasis on information security appears to be appropriate in these two areas:

* **Software**

We should ensure that computer program digital code and associated algorithms receive adequate safeguarding. Increasingly, system update and adaptability are achieved through system software. Computer code now defines and documents system characteristics, performance, decision making or supporting algorithms, and operational employment. Protection is essential to prevent data and advanced design features from being copied and used against our interests, and to prevent knowledge of their specific characteristics from aiding an adversary operationally to defeat or degrade US capabilities. These concerns stem not only from the sensitivity and transportability of information itself, but also from the fact that software is the critical path in system development because it is complex and highly labor-intensive. Availability of such critical programs can cut years off system development times.

* **"Obsolete" Technology**

We must guard against releasing technology and system designs no longer used in US programs but which would give hostile third-world opponents significant advantages in regional and local conflicts, contrary to our interests. A case in point is the success of Iraq in reverse engineering of nuclear weapons using "obsolete" US data.

Total Quality Management Education and Motivation Program

The single, most popular recommendation for improving security programs emphasizes making individuals accountable for their decisions and actions. This approach has merit if it is kept within common sense bounds. It can bring about improvements in limiting the amount of information that is classified by OCAs and derivative classifiers, who are personally responsible for making and applying classification decisions.

Regrettably, however, individual responsibility for the dissemination of information has become much harder to pinpoint, for obvious reasons. Oral and electronic means of communication are rapid and do not show loss of information or reveal signs of having been disseminated. Trying to place individual blame for compromised or lost information can easily lead to scapegoat actions, and accountable personnel realize this. The danger of increasing personal accountability is that it could be a hollow threat at best, and can become an uncontrollable danger at worst. Draconian measures to punish individuals might even serve as a disincentive for responsible conduct in dealing with classified information. Even with the biggest stick we can not guarantee apprehension of the discloser.

Why not use a carrot, instead, to enlist cooperation, stressing how to handle typical safeguarding situations that arise in the workplace? People generally respond better to positive reinforcement of their successful implementation of desirable procedures than to potential punishment for wrongdoing.

Citing Rather than Quoting

Another approach might entail requiring written originating agency release for any of its classified information that another agency wishes to quote, reproduce, or use in any way. To illustrate, I would compare it to citing sources in the bibliography of a formal treatise. Readers could be referred to the source document(s) where the classified information would be located. For contractors, specific authorization would be required to include classified information that the firm did not originate or that did not appear on its Security Classification Specification. Such controls might reduce the amount of national security information distributed beyond the original recipients.

Such a recommendation is not as ponderous as it might first appear. In many

current papers, reports, and briefings, classified information appears to be virtually gratuitous. Once a paper or presentation becomes classified, there is little incentive to limit the amount of classified information therein. Sensitive information can add an air of authenticity, and offers a convenient reason to restrict dissemination of all other information in a document.

Special Access Program Oversight

Another favorite target of critics is special access programs (SAPs). Some even recommend drastically reducing the number of SAPs by arbitrarily terminating a certain percentage, and then severely restricting formation of new ones through a cumbersome bureaucratic review process. To the degree that extra security is essential for protecting specified official information, reducing SAPs may actually be counterproductive. No one seems to be asking why the standard rules and measures are inadequate, and what has happened to enforcement of the need-to-know principle.

Regardless of whether there are fewer or more SAPs, however, responsible oversight must exist. The most productive solution would be to develop an effective, efficient means of ensuring adequate oversight without violating the need-to-know for the most critical scientific, technical, and intelligence information.

As a means of achieving oversight in general and for SAPs in particular, one suggestion might lead toward a workable arrangement. An OCA could designate three- or four-member ad hoc teams to conduct oversight of specific programs, using representatives from defense or military department acquisition, comptroller, and requirements or testing organizations. Each team must have full access to its program or SAP and would establish permanent liaison with the program manager and cleared congressional staff point of contact. There are costs associated with any such scheme, but the point is that indirect and direct oversight buys credibility for the security requirements.

Conclusion

Just as there was an enthusiastic rush to reallocate money perceived as a "peace dividend" following the collapse of the Berlin Wall, there is now a predictable interest in reducing our security "overhead" because of a perceived reduced threat. Those with experience and knowledge of the situation understand that protecting national security information remains critical. The wholesale dissolution of existing security structures most certainly will lead to unprecedented compromise of information that is vital to our future. Whatever actions the Government takes should be based on a realistic and informed assessment of the attendant costs and risks.

David B. Fell, Jr. is an engineering consultant with more than thirty years of experience in defense systems engineering and analysis and associated security considerations, for both national and international programs. He has supported the Office of the Secretary of Defense as well as the Army, Navy, Air Force, Marine Corps, US Postal Service, US Weather Service, the Exxon and Xerox Corporations, and a number of laboratories.

National Industrial Security Program Impact on Information Systems Security

Gerald L. Kovacich, CFE, CPP,CISSP

On 6 January 1993 then-President George Bush signed an executive order establishing the National Industrial Security Program (NISP). The NISP is a result of a lot of hard work by both Government and contractor industrial security personnel to come up with a consistent program for protecting US classified information. Key concepts of the NISP are to control costs of protecting information, to manage risk, and to safeguard information the same way by both parties to industrial contracts.

The purpose of the NISP is to safeguard classified information that may be released or has been released to current, prospective, or former contractors, licensees, or grantees of United States agencies. This does not include individuals under personal services contracts.

In general the executive order, which took effect immediately, requires that:

1. classified information be protected in an equivalent manner by contractors, et al., as it is by the Executive Branch;

2. the program promote the technological and economic interests of the United States; and

3. the NISP serve as a single, integrated, cohesive industrial security program in an effort to reduce redundancies, overlapping, and unnecessary requirements.

Policy direction will come from the National Security Council (NSC), while the Director of the Information Security Oversight Office (ISOO) will be responsible for

implementing and monitoring the NISP.

The Director, ISOO will:

- Develop directives;
- Provide compliance oversight;
- Review Government agencies' directives and require their modification where they are not consistent with the Executive Order;
- Conduct on-site reviews of implementation of the NISP;
- Report violations of the Executive Order to agency heads;
- Evaluate complaints and suggestions relative to administration of the NISP; and
- Recommend changes and report implementation status to the President through the NSC.

OPERATIONS

The Secretary of Defense in consultation with the affected agencies and concurrence of the Director of Central Intelligence, the Nuclear Regulatory Commission, and the Secretary of Energy, is to issue and maintain the NISP Operating Manual (NISPOM). A recent Presidential action requires the NISPOM to be issued no later than 30 June 1994.

The purpose of the NISPOM is to prescribe specific requirements, restrictions, and other safeguards that are necessary to preclude unauthorized disclosure and control authorized disclosure of classified information.

The NISPOM will require security requirements in all contract phases to include bidding, negotiations, awards, performance, and

terminations, as well as licensing processes and grant processes.

It will also address requirements, restrictions, and safeguards dealing with Special Access Programs (SAPs) and Restricted Data.

The NISPOM directs that managers take into account:

- damage that could be expected from a compromise;
- threats to the information; and
- costs of the requirements, restrictions, and safeguards.

Where possible, the classified information must be protected the same way, whether the information is in the hands of a contractor or the Government agency.

OPERATIONAL OVERSIGHT

The Secretary of Defense (SECDEF) is the Executive Agent for inspecting and monitoring contractors for compliance with the NISPOM. SECDEF will also be responsible for NISP implementation in other agencies, based on mutual agreement. The Secretary of Defense is also responsible for standardization, including forms.

The Director of Central Intelligence (DCI) retains authority over Sensitive Compartmented Information (SCI), but can enter into agreement with the SECDEF to act on behalf of the DCI for inspections and monitoring of contracts. The SECDEF can provide similar services to the Secretary of Energy and the Nuclear Regulatory Commission.

IMPLEMENTATION

Each agency head of the Executive Branch of the Federal Government must appoint a senior official to direct and administer that agency's implementation and compliance with the NISP.

The agency head is charged with:

- issuing directives consistent with the NISP;
- taking corrective actions when a violation occurs; and
- accounting for the costs associated with the NISP and reporting them to the Director, ISOO and subsequently to the President.

The SECDEF will, in coordination with other agency heads, amend the Federal Acquisition Regulation (FAR) where necessary to be consistent with the NISP.

Where feasible and economical, current contracts and licenses will be modified to be consistent with and under the operation of the NISP.

THE NATIONAL INFORMATION SECURITY PROGRAM OPERATING MANUAL

The NISPOM will replace the *Industrial Security Manual for Safeguarding Classified Information, DoD 5220.22-M,* commonly referred to as the "ISM," and other Government directives relating to the requirements for protecting classified information.

A draft of the NISPOM is currently being circulated for review and comments. Chapter 8 of the NISPOM and Chapter 8 of the ISM are both entitled, "Automated Information Systems (AIS) Security."

Since the requirements for protecting classified information on automated systems are generally based on the need-to-know, individual accountability, access control, and audit trails of significant events related to the AIS, there probably will be little change in that regard. However, there are significant differences between the ISM and the NISPOM in its current draft form in several key areas.

The structure of the chapter and the writing style are both improvements over the ISM version. Additionally, the requirements are

written in such a way as to:

- provide clearer guidance;
- separate them into two sections: "Administration and Management" and "Processing and Operations;"
- leave less room for interpretation -- more importantly, avoid misinterpretation by those who must use it.
- use a more comon - sense approach, which employs risk management for determining automated information protection, instead of using measures because "the ISM says so;"
- include appendices which provide:

A. a standard Practice Procedure (SPP), which is used to document the security and use of the AIS and is the basis for the systems approval. It also includes some very good audit trail records. This Government standardization of a SPP format is long overdue. It should provide consistency and be used by all Government agencies, instead of each agency (and even each contract of the same agency) using a different format based on the preference of the security officer for the particular contract.

B. direction related to Memoranda of Agreement to be used between agencies where the AIS are networked or shared.

C. a sample Acknowledgement Statement to be signed by AIS users.

D. direction related to partitioned networks. A partitioned network is "a method of implementing a network using Controlled Interfaces (CIs) such as guards and gateways to separate portions of the network into different maximum classification levels, categories, and/or compartments of information."

SUMMARY

The NISP and the NISPOM represent a good start for establishing a uniform information protection program. They concentrate on using a more common-sense approach of standardization, protecting the information the same way, regardless of whether it is held by the contractor or the Government agency; and working more as a Government-contractor team instead of developing an adversarial relationship.

I hope that security professionals on both sides of the contract continue to build on this success and work more as a team. I also hope that the "not invented here syndrome" can be eliminated and not allowed to take hold. Similar efforts do not seem to be working as well as expected with the change in other security requirements. Time will tell if this approach will work for the NISP.

Gerald L. Kovacich is the president of Information Security Management Associates and has been an NCMS member since February 1992.

SECURITY POLICY FOR INTERNATIONAL PROGRAMS:

Releasing US Classified Information to Foreign Governments and Protecting US Security Interests

Charles C. Wilson

Security specialists are frequently expert in one or more aspects of the regulations and procedures for protecting US classified and sensitive unclassified information. Security requirements take on a new perspective, however, when this information is provided to foreign governments in accordance with US law and regulation. International agreements add a novel and complex dimension to the work of a growing number of security professionals. For several decades, the US Government has approved the sharing, sale, and transfer of information to foreign entities, including governments, private companies, and the North Atlantic Treaty Organization (NATO). Foreign businesses sign contracts to build classified equipment for several US agencies. Government officials provide security assistance to a number of foreign governments. And US and allied military forces share classified data during joint or multi-national exercises and operations. While these examples illustrate the need for an international information security policy, they merely open the door to a subject that deserves wider attention and better understanding. The future may very well bring a significant expansion of international collaboration, including security assistance and cooperative research and development programs. Thus, as more Government and industry security specialists become involved in such programs, a better understanding of their legal basis and operation will be helpful.

Although security policy for international programs--or "international security" as I use the term--became a major US concern only during the late 1970s, US international programs have a long history. The lend-lease program of World War II is an example of a wartime international program. The NATO agreement, signed in 1949, was a major US commitment to an international cooperative security arrangement during peacetime, and ushered in an era of US commitments abroad. Changing military and economic considerations in the years since 1949 have led to an expansion of our international commitments, but especially over the past 15 to 20 years.

A complete listing of all US international agreements over the past five decades would illustrate their diverse natures and changing purposes. These agreements with many individual nations and organizations have stimulated us to develop a comprehensive US international security policy. This has been one of my major interests as the Director, International Security Programs. (See Figure 1)

FUNCTIONS OF THE DOD DIRECTOR OF INTERNATIONAL SECURITY PROGRAMS

1. Establish National and DoD Policies for the Disclosure of Classified Military Information and Material to Foreign Governments and International Organizations.
2. Administer the Interagency National Disclosure Policy Committee (NDPC)
3. Evaluate the Capability of Foreign Governments and International Organizations to Provide Protection
4. Negotiate General and Industrial Security Agreements
5. Monitor Security Arrangements for Security Assistance and Arms cooperation Programs
6. Conduct Liaison with Foreign Government Security Officials

FIGURE 1

In 1976, Congress passed the first of a number of laws which require that we cooperate with our NATO allies in military systems development. Standardization and interoperability thereby became key terms used by those engaged in defense systems development work. The first law encouraged the Department of Defense (DoD) to inititate cooperative programs with our NATO allies, and identified funds for pursuing them. Subsequently, an amendment extended the program to include other close allies outside NATO, such as Israel, Australia, Korea, and Japan. While international agreements on these programs were being drawn up, several short-comings of current US international security policy became clear:[1]

1. Little experience was available to guide the unique security requirements related to international cooperative programs that the US was entering into;
2. The security arrangements necessary for international programs were sometimes more complicated than those associated with domestic programs; and
3. Even though the DoD had established security procedures for conducting international programs, these were not necessarily compatible with the security procedures of other governments.

Over the past eighteen years, US officials have worked toward overcoming these deficiencies.This discussion will focus on the legal and policy basis for the two fundamental aspects of international security: The decision whether information should be disclosed, and the security arrangements developed to ensure program

security protection. I hope to make clear the critical nexus that exists among US information disclosure and technology transfer, the National Disclosure Policy (NDP), and the International Traffic in Arms Regulations (ITAR).

AUTHORITY FOR INTERNATIONAL SECURITY PROGRAMS
1. Arms Export Control Act (AECA)
2. Executive Order (EO) 12356
3. National Security Decision Memorandum (NSDM) 119 (National Disclosure Policy)
4. Director of Central Intelligence (DCI) Directives

FIGURE 2

FOREIGN DISCLOSURE

The security policies and procedures for international programs are based on law (the Arms Export Control Act), Executive Order 12356, National Security Decision Memorandum (NSDM) 119, and Director of Central Intelligence (DCI) Directives (Figure 2). This discussion will address only the first three because they are essential to understanding US policy for disclosing official information to foreign entities. They also provide the basic authority for the security requirements of most international programs. The DCI Directives provide details on related intelligence disclosures, but they do not change basic policy and are classified, so they obviously cannot be discussed here.

Arms Export Control Act

The Arms Export Control Act (AECA) governs the export of defense articles and related technical data. It covers both commercial and Government programs, including certain cooperative programs. The Act is implemented by the Department of State through publication of the International Traffic in Arms Regulation or ITAR, which contains the list of export-controlled articles, or the "Munitions List." The basic premise of the Act is that foreign sales of defense articles shall be consistent with US interests and support world peace. To ensure that such is the case, the Act requires the President to assure the Congress that any proposed export of US defense articles or technical data meets this condition. The President also certifies that a prospective recipient foreign government has agreed to these three basic principles:

1. Title or possession of the articles or data will not be transferred without prior US Government consent;
2. Articles or related technical data will not be used, and the foreign recipient will not permit them to be used, for other than the purpose for which they were furnished without prior US Government consent; and
3. The recipient government will provide substantially the same degree of security protection for classified information as that provided by the US Government.

The AECA provides the legal basis for most international defense programs and their related security requirements.

Executive Order 12356

Executive Order 12356 establishes the national security information program for the Executive Branch. It specifies what information may be classified, who is authorized to classify it, and contains basic rules for protecting, downgrading, and declassifying it. Section 4 of the Order reveals the essence of what security professionals really need to know about access to classified information and foreign disclosure decisions:

- First, the Order directs that classified information may not be released outside the Executive Branch unless it has been determined that the recipient will provide equivalent protection.

- Second, Section 4 requires that NSI may be released only after the holder determines that the intended recipient is trustworthy.

- Third, even when the first two conditions are met, access to the classified information must be esential to accomplish a lawful and authorized Government purpose. For example, the foreign release of a classified system must for a government purpose, not to benefit commercial interests. The Government might permit the release of classified information to support the sale of classified equipment to a foreign government to further US policy objectives or to increase the military capability of a key friendly or allied nation.

Basic to understanding these first three points is a recognition that classified information is official US Government information, a national asset. Therefore, the decision to grant foreign access must be made only by designated US officials. And, as discussed later, classified information must be released to a foreign government and not to foreign contractors or foreign

persons. The reasoning should be clear: The required assurances of protection come from the foreign government, which has legal jurisdiction over the ultimate authorized foreign recipient; the US can determine whether that government has the capability to protect a defense article or information; and we can judge whether the foreign government is trustworthy. As noted later in this article, that government is held responsible for protecting the information.

- Fourth, the Order mandates that the originator of the classified information must approve further dissemination; this is often referred to as the "third agency" rule.

- Fifth and finally, there is reciprocity of protection because the President has stipulated that the US must protect foreign government information, both classified and unclassified, if it is provided to us in confidence. I will discuss this in more detail later.

United States National Disclosure Policy (NDP)

Turning next to the National Disclosure Policy, I will first review the organization of the Executive Branch for carrying out the policy; then discuss NDP-1, the implementing document for NSDM; and finally, outline the basic principles of NDP-1 derived from NSDM 119.

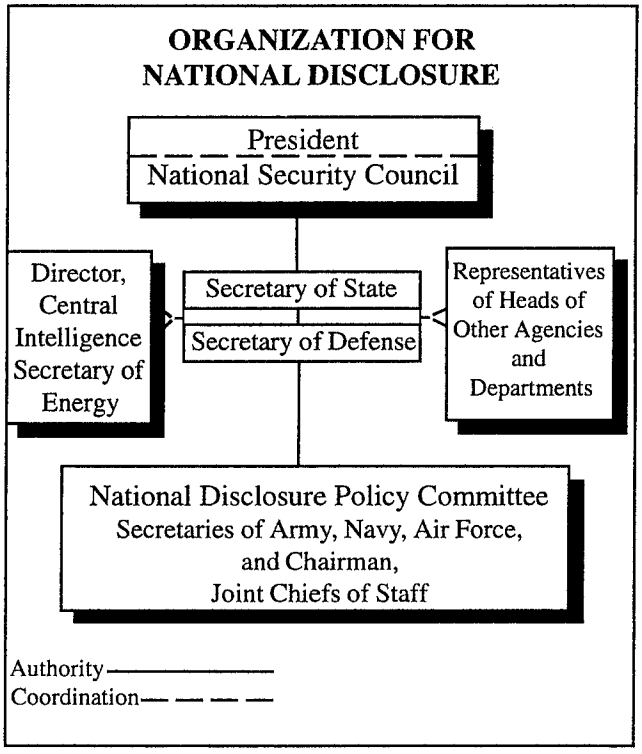


FIGURE 3

Presidential authority and organizational relationships are shown in Figure 3. NSDM 119 charges the Secretaries of State and Defense with implementing basic policy. In furtherance of their responsibilities, the two Secretaries have established the National Military Information Disclosure Policy Committee, or NDPC, to promulgate and oversee the interagency policy for controlling disclosures, and to rule on requests for exceptions to that policy.[2] The Deputy to the Under Secretary of Defense (Policy) for Policy Support represents the Secretary of Defense and chairs the NDPC.

The NDPC consists of general and special members. General members have an interest in and vote on all issues that come before the committee. They include representatives of the Secretaries of State, Defense, Army, Navy, and Air Force and the Chairman of the Joint Chiefs of Staff. Special members have an interest in specified information controlled by the NDP and in issues of concern to them. For example, intelligence community members participate when the disclosure of intelligence comes before the committee. They also make significant contributions when the NDPC addresses the capability of a foreign government to protect US classified information. Special members include representatives of the DCI, the Defense Intelligence Agency, the Department of Energy, and the DoD Offices of Acquisition and Technology, Policy, Atomic Energy, Ballistic Missile Defense Organization (formerly Strategic Defense Initiative Organization) and Command, Control, Communications and Intelligence (C3I).

National Disclosure Policy-1

NDP-1, issued by the Secretary of Defense with the concurrence of other departments and agencies, implements NSDM 119 within the Executive Branch. It delegates disclosure authority for classified US military information to the heads of departments and agencies with jurisdiction over the specific information at issue, based upon five disclosure principles stated in NSDM 119.

Basic Principles of the National Disclosure Policy

Many of the NDP principles are similar to the requirements of the Arms Export Control Act and Executive Order 12356. This is not surprising because classified information is a national asset; it may not legally be shared with a foreign government or international organization unless release results in a clearly defined benefit to the US Government. And in

the words of Executive Order 12356, release must be for a lawful and authorized government purpose.

This leads to discussion of the five basic criteria that must be satisfied before US classified information may be authorized for release to a foreign entity:

1. Release must support US foreign policy toward the intended recipient government and other governments in the region.
2. Release must not jeopardize US military security. This is probably the most difficult of the criteria to satisfy and warrants some elaboration. It causes us to do a cost-benefit analysis, or an advance damage assessment. The proponent of release must place a value on the information and evaluate possible damage to US military capability if the item, information, or technology is compromised, regardless of the intended recipient. This is an especially important evaluation for equipment sales because it addresses concerns about the technology upon which the system is based. At times, industry will be consulted in part because we may consider possible system modifications or release of an export version of the basic equipment. It is often useful to examine the foreign availability of similar systems and technology and to determine the susceptibility of a system to reverse engineering. US firms applying for an export license help both industry and Government by providing information that satisfies this criterion.
3. The recipient government must possess the capability and demonstrate intent to provide substantially the same degree of protection as that provided by the US Government.

Capability is evaluated in two ways:

- First, we seek the US intelligence community's assessment of the recipient government's security program. We analyze its history in protecting information, its pertinent laws and regulations, and look for recent trends to improve or backslide.

- A second way of evaluating capability involves assembling a team of security experts from DoD and other Executive Branch agencies to review the program with security officials of the foreign country. The team will visit military and industrial facilities for an on-scene evaluation of that nation's implementation of its own security programs. It is important to note that these visits are not inspections, and they are reciprocated. Many foreign government security officials have visited DoD facilities in the US for this purpose. The visits not only satisfy our statutory and regulatory requirements, but they also result in better mutual understanding of security procedures and facilitate negotiation of standing security agreements.

Intent of a foreign government is to protect US information is established by negotiating a security agreement. We have two types of agreements: General (See Figure 4) and Industrial (See Figure 5). The US DoD prepares and usually negotiates both types, but a DoD official signs the Industrial agreements while the Department of State approves and signs the General agreements. Both types satisfy the security requirements of the Arms Export Control Act and the requirements of Executive Order 12356.

- Under a General Security Agreement--whether called a General Security of Information Agreement (GSOIA) or General Security of Military[3] Information Agreement (GSOMIA), both countries make a commitment to protect classified information provided by the other government, and they agree to refrain from retransferring or using the information for other than the intended purpose, except with the consent of the originator.

KEY FEATURES OF GENERAL SECURITY AGREEMENTS
(GSOIA and GSOMIA)

- Executive Agreement, Not a Treaty
- Accomplished via Diplomatic Channels
- Does NOT Commit Governments to Share Information
- Does Commit Governments to Protect Any Information Shared
- Prohibits Release to Third-Country Person, Firm, or Government
- Recipient Agrees to Provide Substantially Same Protection
- Permits Use of Information Only for the Purpose Specified
- Guarantees Respect for Private Rights
- Transfers are Government-to-Government
- Restricts Access to Need-to-Know Basis
- Requires Reports of Compromises
- Establishes Reciprocal Security Visits
- Encompasses Basic Security for Releases to Industry

FIGURE 4

Furthermore, General agreements require the reporting of all compromises and transfers of classified material through government channels. We currently have about 50 General Security Agreements.

INDUSTRIAL SECURITY AGREEMENT

- Negotiated by DoD as an Annex to GSOIA or GSOMIA
- Contains Implementing Procedures for Contracts and Other Government-Approved Arrangements Involving Access to Classified Information by Foreign contractors:
  - o Information Handling
  - o Security Classification Guidance
  - o Security Requirements Clause
  - o Visits
  - o Security Assurances
  - o Responsible Agency or Office

FIGURE 5

- Industrial Security Agreements are negotiated with foreign governments whose industries participate in US defense programs, such as the countries with which DoD has a reciprocal procurement agreement or a defense industrial cooperation agreement. Industrial agreements are basically procedural documents that describe the security procedures used by a foreign industry involved in a classified US defense program. Examples of issues addressed in an Industrial agreement include contract classification guidance, security clauses in contracts, industry visits, and security assurances for personnel and facilities. We have 20 Industrial Security Agreements in place.

4. Disclosures of classified information to foreign governments must also result in benefits to the United States. This criterion satisfies the access provision of Executive Order 12356 which requires that access be in pursuance of a lawful and authorized Government purpose. The benefit may be political or military in character, and it may mutually benefit the United States and a close ally by supporting defense interoperability and standardization.

5. Finally, disclosure must be limited to that information necessary to satisfy the purpose for which it is authorized. For example, if the purpose is to sell a weapons system, the recipient government must be provided the information required for its operation, maintenance and training. But information needed to build it certainly will not be released. Related research and development data or manufacturing know-how also probably will not be released. In some cases, the prescribed data will be excised from documentation before it is transferred.

Delegation of National Disclosure Authority to DoD Components

The DoD receives visit requests from more than 300,000 foreign officials each year. Many of these visits involve access to classified information, resulting in some 10,000 to 15,000 foreign governments requests annually for classified documents. Some of the requests encompass up to 200 individual items. The NDPC cannot possibly review this number of requests and render decisions on each case. Therefore, disclosure authority has been delegated to the Military Departments and other agencies that originate the information. Briefly, the arrangements that have been made to simplify and standardize release decisions are as follows:

- The NDPC delegates authority by security classification level for each of eight categories of classified military information, listed in Figure 6. The DoD Components appoint officials in writing to control foreign disclosure decisions. They must first determine that it is information over which they exercise classification jurisdiction. They must also confirm that each proposed release satisfies the NDP disclosure criteria mentioned earlier. Then, they must determine if the classification level falls within the delegated level for the category of information in question. Finally, they must coordinate these decisions with other agencies which have an interest in the system or information at issue; for example, a radar system containing technology common to each Military Department would be coordinated with each of them.

- Decisions are made on a case-by-case basis. If any criterion is not satisfied or information exceeds the authorized level, the proposal must be denied or the proponent must obtain an exception to the NDP for its release. The Secretary and Deputy Secretary of Defense and the NDPC may approve exceptions to the policy. The release of US classified information to a foreign entity requires a positive decision in each case that disclosure will result in a benefit to the United States that outweighs any damage that might occur from compromise.

Experience led us to realize that many foreign governments have solid security programs. Therefore, disclosures usually can be approved in categories 1 and 2 to those countries because they normally maintain it

under government control. For those countries with weak industrial security programs, the NDP will

EIGHT CATEGORIES OF CLASSIFIED US MILITARY INFORMATION

1. Organization, Training and Employment of Military Forces--general information that is not specific to any one system, such as air defense training or unit organization and deployment.
2. Military Material and Munitions and the information needed for its operation, maintenance, and training. This category pertains to systems that are in, or have completed, production. Most military equipment is unclassified, but, for some equipments certain operations, maintenance, training, and employment information is classified-- such as susceptibility to countermeasures and system capabilities. Foreign disclosure decisions require looking at supporting information that will be released if the sale is approved, especially when an unclassified weapon system is involved. If all information cannot be released, the sale probably will not be approved.
3. Applied Research and Development Information
4. Production Information (design and manufacturing know-how).
5. Combined Planning and Guidance (JCS-type information)
6. US Order of Battle Information
7. North American Defense Information
8. Military Intelligence (collateral information only)

FIGURE 6

delegate lower levels of disclosure authority in categories 3 and 4. In some cases, we may impose additional security measures even if we have a security agreement with the recipient country; these will be included in the program agreement or an annex to a Letter of Offer and Acceptance, if sensitive information may ultimately be released to industry in that country.

Figure 7 illustrates how authority may be delegated for disclosures of specific information in each of the eight categories to nominal countries A, B, and C. Such authorization makes possible a favorable release decision by a DoD Component, for example, but does not mean that the Component must decide to share, sell, or exchange specified classified military information in that category.

Foreign Disclosure Decision Making Process: The NDP Outlines Procedures, But Does Not Make Release Decisions

There is an important point to remeber about disclosure decisions and the NDP: The NDP alone is not the basis

DELEGATION OF NATIONAL DISCLOSURE AUTHORITY
(Example of NDP-1 Charts)

		COUNTRY		
	CATEGORY	A	B	C
1.	Organization, Training, and Employment of Military Forces	S	C	
2.	Military Material and Munitions	S	C	
3.	Applied Research and Development Information and Material	C		
4.	Production Information			
5.	Combined Military Operations, Planning, and Readiness			
6.	United States Order of Battle			
7.	North American Defense			
8.	Military Intelligence	TS	S	C

FIGURE 7

to oppose or deny a proposed disclosure of classified information! The NDP outlines procedures and criteria that are, for the most part, based on the provisions of the Arms Export Control Act and Executive Order 12356. Intelligence disclosures are based on intelligence community directives. The NDP establishes the framework for making disclosure decisions based on the Act, EO 12356, and other directives and policies. Moreover, there are provisions in the NDP for exceptions if the disclosure will result in a clearly defined benefit to the US Government that outweighs any damage that might result from compromise.

SECURITY ARRANGEMENTS FOR INTERNATIONAL PROGRAMS

Once a decision has been made to disclose classified information to a foreign government, the National Disclosure Policy requires that certain security conditions must be satisfied before a transfer can occur. These conditions are essentially the same as those contained in the Arms Export Control Act regarding use, re-transfer, and security, and in EO 12356. Moreover, transfer must be made using designated representatives through government-to-government channels, and signed receipts are required. The discussion that follows briefly examines the other half of international security programs: the specific security arrangements involved.

DoD is responsible for ensuring that classified information is transferred to foreign entities only under the terms and conditions outlined in US laws and regulations, regardless of the type of program by which it is conveyed. (See Figure 8) Government and commercial exports are conducted in accordance the same principles. While it may be relatively simple to make a decision to disclose US classified information to

a foeign entity, a considerable amount of security activity must take place to carry out that decision. That activity encompasses marking, receipts, packaging, clearance validation, verification of release authorization, and transmission.

PROGRAMS THAT INVOLVE DISCLOSURES

- **Direct Commercial Arrangements:**
  - Direct Commercial Sales
  - Manufacturing License or Technical Assistance Agreements
  - Plant Visits
- **Government-to-Government Arrangements:**
  - Personnel Exchange Arrangements
  - Information Exchange Agreements
  - Foreign Military Sales
  - Cooperative Research, Development, and Production Agreements
  - Foreign Visits

FIGURE 8

The Multinational Industrial Security Working Group, or MISWG, offers an excellent example of how we have worked with foreign governments to develop security rules and procedures. MISWG grew out of 1986 discussions with representatives of NATO member nations concerning security procedures for international cooperative programs that are not managed by NATO. They agreed to convene annual meetings to resolve security-related problems through adopting standard procedures that would facilitate the exchange of technical data.

MISWG seeks to identify security problems and develop, coordinate, and recommend standard procedures for non-NATO cooperative programs. These are programs not commonly funded or managed by NATO organizations, even though they may be conceived in a NATO group. Such programs are subject to national laws and regulations rather than NATO regulations. Standardization is to be accomplished in a manner that does not require the participating nations to modify their existing laws. All NATO member nations except Iceland take part in the MISWG effort.

As of 1993, the Senior Security Officials of each country had approved standard rules or procedures in the following areas:

- Security clauses for international agreements
- Visits
- Transportation plans, including format
- Hand-carrying classified material
- Controlled Unclassified Information
- Restricted Information
- Exchanging facility security clearances and security assurances
- Use of secure communications
- Security education requirements
- Format for recording and exchanging information on participating contractors and key personnel, such as security officials, who are involved in an international program
- Program Security Instruction--a form of standard operating procedure that consolidates procedures for handling classified information and other program information involved in a cooperative program. It may also include other MISWG procedures, such as the transportation plan or hand-carry procedures.

MISWG procedures have been distributed to those offices within each DoD Component that are involved in international programs. The Defense Investigative Service has provided them to its field offices for use by Defense contractors.

Charles C. Wilson is Director for International Programs in the Office of the Deputy Under Secretary of Defense for Security Policy, and serves as Executive Director of the interagency National Military Information Disclosure Policy Committee.

---

[1] It was also clear that the US would have to resolve the policy and procedural differences if we hoped to do business with our allies. Out of that effort to standardize and achieve reciprocity in security policies came an organization known as the Multi-national Industrial Security Working Group (MISWG). Over these years of discussion and extensive negotiations, the MISWG has been able to produce agreement on standard security procedures among the participating nations. This painstaking process should not be taken lightly nor its results whimsically overturned. Based on my several decades of experience, I cannot find any rational basis to support recent suggestions that the US should relax our rules for security accountability or abruptly eliminate the three levels of security classification and protection. We already face significant challenges in trying to handle international secuirty matters with our allies, many of whom use four levels of classification. Many of our allies also operate with procedures they adopted from US programs that have been in place over the past 30 years.

[2] It will come as no surprise that certain information, shown in Figure 9, is outside the purview of the NDP. The foreign release of such information is governed by other laws, Executive Orders, National Secuirty Council Directives, and agency

policies. In some cases, separate committees or offices make the decisions whether to release this information. The NDPC may be required to consult with these other officials when considering the sale of certain military equipment when such information is required to support the sale.

For example, a foreign government may wish to have communications equipment hardened against an electromagnetic pulse threat before purchasing it; in this instance, the Joint Atomic Information Exchange Group or the Department of Energy may coordinate on the approval to release the equipment for sale. Similarly, the prospective sale of a radar warning receiver that is programmed with intelligence threat data may be coordinated with the SIGINT Committee for approval. DoD Components are encouraged to coordinate such concerns with the appropriate agency or committee prior to concluding discussions with foreign governments regarding a sale. Then, if it becomes necessary to submit a request to the committee for an exception to the NDP, the Component is obligated concurrently to submit evidence that all required coordination has been accomplished. On occasion, the lack of coordination has caused delays in approving an industry license application or a proposed foreign military sale.

INFORMATION OUTSIDE THE NATIONAL DISCLOSURE POLICY

- Atomic Energy Information
- National Intelligence
- Counterintelligence Products/Programs
- Signals Intelligence (SIGINT)
- Communications Security (COMSEC) Information and Material
- Strategic Planning and Guidance

FIGURE 9

[3] Classified military information is information requiring protection in the interest of national security as described in EO 12356 and which is owned by or under the control or jurisdiction of theDepartment of Defense or a DoD Component.

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]

TITLES AND AUTHORS OF PREVIOUS *VIEWPOINTS* ARTICLES

NCMS Viewpoints, Volume II, 1992 (Published October 1992)

TITLES AND AUTHORS OF PREVIOUS *VIEWPOINTS* ARTICLES

NCMS Viewpoints, Volume I, 1993 (Published February 1993)