VIEWPOINTS

A PUBLICATION of the NATIONAL
CLASSIFICATION MANAGEMENT SOCIETY
VOLUME 1, 1993

ISSN-0009-8434

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

VIEWPOINTS

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

NCMS members deal with security confronting the Government and industry today and into the future. For example, we must cope with technology not only as an object of classification but also as a tool for managing an unknown but vast and growing quantity of classified information.

We recognize the need to protect information about U.S. national defense and foreign relations against premature disclosure, even while adapting to new operational and international realities that call into question the traditional security protection afforded so much Cold War subject matter. Nevertheless, the task still remains to safeguard national security information (NSI) "as long as required by national security considerations." [Executive Order (EO) 12356, Section 1.4(a)]

Most of us can defend, and have done so, policy in EO 12356 to protect specific NSI for as long as necessary--that is, for extended periods of time. What demands our attention at present, however, and will become more insistent, is the burden of storing enormous quantities of classified records for 30 years or longer, and how to cope with the complex and costly problem of declassification to serve legitimate public purposes.

Classification management has a historical dimension that cannot be ignored. To define the boundaries, and discuss the future of our classified national storehouse, we sought the views of Viewpoints' first guest editor, Dr. Don W. Wilson, Archivist of the United States. It is clear from his account that, even if no more files were accessioned, present staff of the National Archives (NA) would require decades to process the classified records using current guidelines and procedures. A similar challenge confronts the Department of State, which is charged by law with publishing, within one year after they reach 30 years of age, documents relating to the foreign relations of the United States. Available resources are so limited as to preclude either the NA or the State Department from complying fully with the declassification review requirements imposed by EO 12356 and statute.

Jeanne Schauble, head of the NA declassification division and our point of contact with Dr. Wilson, reports on a related timely topic: How does classified information comes to be in the "private" papers of senior officials who have left Federal Government service? This is a fact of life dating back to the earliest days of security classification. It places national security information at risk when adequate Government controls are not maintained over it. Citizens may well puzzle whether this is legal or a political problem, or both. Regardless of the answer, like death and taxes this issue will remain with us and probably intensify like the recent east coast "storm of the century," at least every four years.

James J. Bagley agreed to have his speech adapted as an article dealing with unclassified official information. It seems fair to characterize his topic as tragicomedy with implications for virtually every U.S. agency, department, and other element that produces information of interest to some part of the public. Hence, the reader will find humor to lighten up the discussion, starting with a well-known comedy routine by Abbot and Costello. The message, however, is most sobering.

Directly related to Jim Bagley's lead article, as many members are already aware, the Export Administration Act (EAA) of 1979 expired on 30 September 1990. This Act gave the Department of Commerce authority to control the export of certain dual-use technology that would lead to the proliferation of nuclear, chemical, and biological weapons.

Commerce has been operating under emergency authority of a Presidential executive order, leaving officials concerned about possible legal challenge to Government actions. To remedy this predicament, the House of

Representatives voted in February to reauthorize the EAA through 30 June 1994 with $42.8 million. This temporary measure will buy time while Congress "totally rewrites" the Act. Representative Toby Roth (R-Wisc) envisions new legislation to codify an export policy that controls only what has to be and can be controlled, but at the same time allows U.S. industries to compete in world markets.

Richard A. Black examines international concerns and identifies a trend toward greater participation by foreign nationals in our research laboratories. He proposes several solutions to the attendant security problems that are certain to provoke response from other security professionals, and perhaps a few interested parties outside the normal field of NCMS membership.

Jeanne Bastoni takes sides on the controversial question of whether accountability for Secret documents makes sense in the age of automation, rapid reproduction, and ubiquitous telefacsimile machines. This brief statement only scratches the surface of a debate that reveals more every day about current security practices and vulnerabilities.

Gerald L. Kovacich raises a topic that grows steadily in importance to Government and industry: Protecting and limiting access to classified information in automated databases. Anyone who is unclear about what a "trusted" database system is will quickly find a comprehensive answer here. But the value of this article goes much beyond learning technical computer terminology. It suggests an approach to solving automated systems security problems by drawing upon familiar analytic techniques used for manual systems.

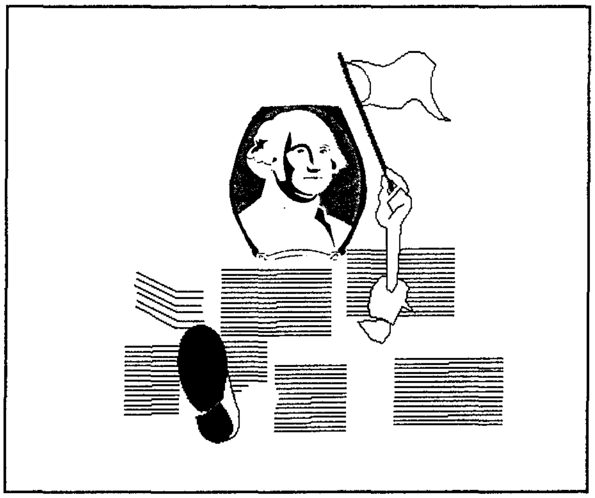
John P. Waller answers the question of what makes an effective security program? His prescription is decidedly proactive and urges security managers to maintain contact with the customer. . . and other key members of the corporate team.

Closely related in spirit is Adam L. Gardner's blueprint for a successful security training program using principles and techniques of total quality management. His skillful illustrations give rapid insight into the systematic approach to a quest for excellence.

As in the previous issue, the titles and authors of previous Viewpoints articles appear at the back. Also a summary of NCMS requirements for submitting articles is again provided on the last page.

Raymond P. Schmidt

Guest Editorial



ENDING THE DECLASSIFICATION LOGJAM

Don W. Wilson
Archivist of the United States

The suddenness, and the finality, with which the Cold War ended continues to astound the senses and jar the emotions of anyone who lived through a significant portion of it. For more than four decades after the Second World War, this fundamental geopolitical and philosophical stand-off between the United States and the U.S.S.R. profoundly influenced the diplomatic relations, domestic politics, intellectual and cultural life, and overall world outlook of most Americans and Soviets alike. Neither a full-scale direct conflict, despite some close calls, nor a relaxed coexistence, although we sometimes approached that, the Cold War was a novel and difficult period for American citizens and policymakers.

"...approximately 10% of our holdings are security classified;...within five years nearly 40% ...will be classified."

But now that period has come to an end, and we must deal with the legacy of the Cold War. For the National Archives, that legacy includes millions of classified records already in our custody and millions more that agencies will ultimately deliver to us. Already, approximately 10% of our holdings are security-classified;* we estimate that within five years nearly 40% of all the textual records we accession will be classified, and increasingly high percentages of non-textual records will also be of this type.

Because of the special nature of the Cold War itself, declassifying these records presents unique challenges that we have not faced before. Both the diplomatic establishment and the intelligence agencies grew in size and importance during the Cold War, and the high stakes for which they played contributed to a heightened desire for secrecy. Military technologies became ever more sophisticated, and the development of new weapons, especially nuclear weapons, resulted in extraordinary security classifications that also meant tight restrictions on information. Newly created multinational organizations brought with them the problem of handling classified information involving other governments. The complexity of Cold War decision-making in general, with its increased use of interagency communication and consultation, added layers of authority and interest. All of these factors pose difficulties when it comes to declassifying Cold War-era records.

"The current declassification process is slow and cumbersome."

The current declassification process is slow and cumbersome. In the absence of specific, automatic declassification dates, the National Archives must try to review classified records systematically while it responds to the requests of researchers to see particular records. Using guidance from the agencies that created the records, trained National Archives specialists

**The National Archives holds many classified records dating back to World War II, and even earlier.*

and paraprofessionals review those materials that would seem to have the highest research interest--and that are most likely to be declassified.

Ideally, the National Archives would work its way systematically through the classified records in this manner. Unfortunately, that is not possible. Since we cannot exceed the authority delegated to us by the agencies that originated the records or impose our own judgment, the kind of guidance we receive from the agencies is crucial. Some of the guidance provided is so broad that we must refer records back to the appropriate agency--often, to multiple agencies--for a decision. Agencies also reserve authority in some or all subject areas, which means they must review any records in those areas. Only some records can be declassified in bulk; the remainder must be reviewed page by page by at least two trained reviewers. The mixture of declassified and classified information in some formats--microfilm, for instance--also can interfere with review for systematic declassification. Moreover, finding aids and indexes can themselves be classified, and typically they can be released only after all the classified information they relate to has been released.

Meanwhile, the National Archives receives from researchers numerous requests for mandatory review of certain security-classified materials that are not undergoing systematic review, as well as many additional requests under the Freedom of Information Act (FOIA). If the National Archives does not have declassification authority for these materials, we must photocopy every page requested and forward the copies to the agency or agencies of origin for a review and determination. The <u>average</u> FOIA request for classified records, I should add, asks for about 1,500 pages. Handling these requests, which are governed by very specific regulations and judicial decisions, often forces the National Archives to set aside its systematic declassification schedule. Limited resources, and the complex nature of the review process, makes declassification slow work, and even then it is not always successful. Delays of several years between the time of request and the release, or denial, of the information are not uncommon.

"Limited resources, and the complex nature of the review process, makes declassification slow work...Delays of several years between the time of request and the release...of information are not uncommon."

Most of the Cold War documentation that the National Archives has already received dates from the period between 1945 and 1960. The relaxation of Cold War tensions and our move to Archives II* means that the National Archives will probably be accessioning many more millions of classified records than we had previously anticipated. Unless we act, therefore, tens of millions of additional records will be added to the backlogs that the National Archives--and its researchers--are already experiencing, just as scholarly interest in the Cold War is increasing.

For all these reasons, I believe that the present declassification process is flawed so badly that it cannot be repaired. Nor <u>should</u> it be.

I support the introduction of a fixed declassification date, so that older materials can be more quickly released without the costly, page-by-page review that is now required. A reasonable fixed date would seem to be forty years: materials older than that would be automatically released; those less than forty years old would be reviewed for possible release, perhaps under more limited restrictions than now exist.

* *Archives II is a new facility under construction on former University of Maryland grounds near College Park north of Washington, D.C. The 1,700,000 square feet facility being built on 33 acres will house approximately 2,000,000 cubic feet of retired records, many of them from the Cold War era. Archives II is scheduled to open to the public and researchers in 1994.*

If necessary, the United States could phase in an automatic declassification system, setting a date a few years hence when all materials more than fifty years old would be released and another date, somewhat later, when the automatic forty-year rule would take effect. Our goal ought to be to have a fifty-year rule in effect by 1998, the 50th anniversary of the Berlin Crisis that did so much to define the Cold War.

When the nations that were our adversaries are now our friends, or no longer exist at all, is there any justification for keeping secret the information about our relations with them four decades ago? If we in the United States do not act promptly, those countries may well release information about these topics before we in a free society do. Is there any reason, given our national financial constraints, to maintain the existing costly declassification process when the reasons for secrecy have for the most part vanished?

"I support the introduction of a fixed declassification date....Is there any reason...to maintain the existing costly declassification process...?"

Only when Cold War records more than forty years old are automatically released for research use will we free ourselves from this burden that must no longer be carried. And only when we have access to these records will we as a society fully understand the national security history of the United States, how our own actions influenced the development of the Cold War, and how it affected us. The American people deserve to have access to this information, now that the reason for keeping it secure has gone. The declassification system that is presently in operation is itself a relic of the Cold War. Just as we are thinking in new terms about the world in which we live, we must think differently about the records that date from the Cold War. The 103rd Congress and a new Administration are likely to come to grips with this issue, and the National Archives looks forward to working with them to see that the American people have access to these records at the earliest practical date.

"The declassification system...is itself a relic of the Cold War."

UNDERSTANDING CONTROLS ON UNCLASSIFIED GOVERNMENT INFORMATION
or
"WHO'S ON FIRST?"

James J. Bagley

The need for controls on the dissemination of unclassified information and technical data is not new. This nation has made efforts to control its unclassified official information for many years. Even George Washington had problems protecting it. The battle over whether to release information, on the one hand, or to withhold it on the other, continues to rage.

I have long contended that the control of unclassified Government information is the most critical problem we now have, or will have in the future. I first expressed this view during my talk in 1967 at the third annual NCMS seminar, an event also marked by a keynote address given by Congressman John E. Moss, father of the Freedom of Information Act signed by President Lyndon B. Johnson on July 4, 1966.

Many readers remember the classic Abbot and Costello baseball comedy routine:

"Who's on First, What's on Second, and I Don't Know is on Third." One biographer called it "Abbot and Costello's immortal confrontation with the laws of logic." And that also characterizes the story of unclassified Government information: a confusing confrontation with logic--or illogic, if you prefer.

In this article I will try, and try is the operative word, to give you a flavor of the logic of chaos, because that describes the situation concerning unclassified official information--pure chaos. Whether deliberate or not, you can make your own judgement, but chaos it is.

I begin with basic definitions of unclassified official and classified information and give origins of the debate over the need to control unclassified information. Next, I present definitions for several other related terms, and propose adopting a pair of descriptive terms by adding modifiers to "unclassified" for the sake of clarity.

Next, I will explore the effects of the definitions on several organizations involved in international trade.

Then, in the context of current world trade and political realities, I discuss what is at stake and the U.S. role in unclassified technology transfer.

Last, I throw it all up in the air and say "I Don't Know." Perhaps this approach offers the possibility of moving our discussion from a state of pure chaos to controlled confusion. Finally, I will offer some suggestions.

Basic Working Definitions

Unclassified is a security classification assigned to official information that does not warrant the assignment of Confidential, Secret, or Top Secret markings but which is not publicly-releasable without authorization.

Classified information is defined in PL 96-456, the Classified Information Procedures Act:

> Any information or material that has been determined by the United States Government, pursuant to an executive order, statue, or regulation, to require protection against unauthorized disclosure for reasons of national security and any restricted data, as defined in paragraph r or section 11 of the Atomic Energy Act of 1954. [42 USC 2014(y)]

This definition is identical with one proposed in the draft National Industrial Security Program Operating Manual (NISPOM), except that the latter does not include the words "or regulation," By adding those two words, one could argue that PL 96-456 gives us a statutory, as well as an executive, basis for the classification of U.S. information. We could thus resolve the longstanding debate as to whether the classification system has a basis in law.

Prior to 1953 the U.S. employed a **Restricted** classification that applied to information withheld from public dissemination. It was cancelled with the issuance of Executive Order 10501 on November 5, 1953.

Despite the cancellation, many people inside and outside Government expressed concern about the tremendous effort being made by the Soviet Bloc to collect U.S. industrial and military information. This concern led to the establishment of the **Office of Strategic Information** (OSI) in the Department of Commerce to provide a central Government office to work with the business community in voluntary efforts to prevent the loss to foreign interests of unclassified strategic data. It was aimed primarily at protecting defense information of the United States. The OSI did not stay in operation very long--it was disestablished in 1957. Note the word "voluntary" in its mission. This was not a sufficient statutory base to limit dissemination of some technical information.

A few years later, in 1960, the **House Committee on Government Operations** issued a report citing 842 Federal statues controlling Government information. The study leading to publication of the report is still pertinent because it led to this finding:

> The subcommittee uncovered case after case of executive officials withholding information without any legal authority.
> ...In other cases, however, executive officials have gone beyond the law to claim 'executive privilege' for secrecy when there is no legal privilege.

So, what's new?

Still later, on January 10, 1963, the **President's Science Advisory Committee** concluded that:

> The panel is aware of the asymmetry that exists between the way the communist and non-communist worlds handle information. We believe, on balance, that our more liberal policy leads to more security, not to less. Nevertheless, we do not believe it in the public interest always to push automatically for more dissemination. Each case must be decided on its own merits.

In 1966 there was an important event, one that still stimulates debate as to its impact on the national security. That was the passage of the **Freedom of Information Act** (5 USC 552 (b)). I will discuss it further later in the context of limitations on public release.

Considerable pressure, much of it political, was brought to bear and the Congress recognized the need to define terms and develop a statutory basis for exempting certain unclassified information from automatic public release. The question at issue was at once both simple and profound:

> **Does information that has been declassified automatically become public information?**

Many people took the position in 1966 that declassification equals public release. The debate on that point is historic and endless, continuing today even in the face of numerous statues which limit or control the dissemination of unclassified data and information. A recent example is the article entitled "The Perils of Government Secrecy" published in the Summer 1992 edition of Issues in Science and Technology magazine.

I have always believed that this debate is healthy. It resembles and extends another closely-related debate about whether there is too much classified information. I firmly believe that any original classification authority or releasing official must have a solid justification for classifying, limiting dissemination, or withholding information. Furthermore, any decision to restrict the dissemination of or to withhold information from public release must be made by an official with authority and be time limited.

In the late 1960s Congress charged that the Department of Defense (DoD) was releasing too much unclassified but critical or sensitive information to the Department of Commerce's National Technical Information Service (NTIS) via the Defense Technical Information Center (DTIC). In 1970 the DoD Director of Research and Engineering established a DoD committee to approve or disapprove the transfer of reports from DTIC to NTIS. I was the chairman of the committee as well as the DoD and Navy representative. The committee had the authority to prevent document transfers and to question the military commander or civilian director why his organization had authorized the release of a particular item to NTIS, that is, to the public.

Our procedure was to call the official and ask him why he had released "Report X." Obviously, he often could not justify the action, but he usually went on the offensive, asking who we were to question his judgement. Our response was to ask him whether he was prepared to defend his decision to his agency as well as to the Secretary of Defense. This approach did get the official's attention. Over time there was a considerable reduction of critical information being released via NTIS. I recommended that our committee be disestablished in 1975.

During this time one vaguely-defined question continued to nag us:

> **How can the Government control dissemination of unclassified technical data?**

The question caused us to focus on the distinction between technical information and technology. There has long been confusion as to what unclassified technical information or technology should be controlled. Resolving this conundrum hinges upon explaining the differences between research and development, test and evaluation, and other efforts that are the precursors to production.

Fred Bucy, then president of Texas Instruments, took the lead in advocating that technology, and not the broader research and development information, must be controlled. His advocacy led to codification of that distinction in law and regulation in what is now called the **Militarily Critical Technologies List**. Next, Congress passed a law to control unclassified controlled nuclear information (UCNI) originated by the Department of energy. Later, another law exempted DoD UCNI from release under the FOIA.

Technological information is identified as a separate category of unclassified information. It is generated during exploratory development, advanced development, and test and evaluation.

Note that the term research does not appear in this definition. Research produces knowledge, which, in turn, creates the need for development and technological information. Development also produces knowledge that can be applied to a specific defense problem or other defined need.

Other statues added to our understanding and confusion about unclassified official information:

> * The Classified Information Procedures Act of 1980 (PL 96-456, 94 STAT. 2025 referred to above), among other things provided an interesting definition of classified information.
>
> * DoD Instruction 5210.74, Subject: Secretary of Defense Contractor Telecommunications, provided a new definition of that term plus examples of other unclassified information to be controlled.
>
> * The COMSEC Supplement to the Industrial Security Manual for Safeguarding Classified Information, DoD 5220.22-S-1,

Examples of Limitations on Unclassified Information

- o Freedom of Information Act (5 USC 552)
- o Unclassified Controlled Nuclear Information (20 CFR 1017.1)
- o DoD Unclassified Controlled Nuclear Information (10 USC 128)
- o International Traffic in Arms Regulation (22 USC 2778 (a)
- o Export Control Administration Regulation (FEB 1992, EAA of 1979) Dual-Use Information
- o Unclassified National Security Related Information (DoD 15210.74)
- o Sensitive but Unclassified Information (COMSEC/ISM)
- o Withholding of Unclassified Technical Data from Public Disclosure (DoDD 5230.25, PL 98-94) (10 USC 130)
- o Militarily Critical Technologies List
- o Distribution Statements on Technical Documents (DoDD 5230.24)
- o Limited Official Use Information
- o Computer Security Act of 1987 (PL 100-235) Sensitive Information
- o Drug Enforcement Administration Sensitive Information
- o COMSEC Supplement to the DoD ISM Sensitive Information and Technologies

Figure 1

gave us still another definition of sensitive but unclassified information.

* At the same time, the Export Administration Act of 1979, with the most recent regulation being issued in February of 1992, also defined unclassified information.

* The International Traffic in Arms Regulation, 22 USC 2778 (a), subparagraph 204.404-70, provided a new definition under the additional contract clause subparagraph: "Disclosure of information in solicitations and contracts when the contractor will have access to or generate information that may be sensitive or inappropriate for release to the public."

As you can see, we are awash in definitions. If you are not already confused, you should be.

Proposed Descriptive Terms for Unclassified Information

It may surprise some readers to learn that the DoD has no official definition of Unclassified in DoD Regulation 5200.1-R (Information Security Program Regulation), DoD Manual 5220-22-M (Industrial Security Manual for Safeguarding Classified Information), or DoD Directive 5220.22 (DoD Industrial Security Program). The initial draft NISPOM sets forth a proposed definition that, to me, is misleading. So, to make discussion clear, I will use several old terms which modify Unclassified. The distinction shown here is currently out of fashion, but I believe that it is still useful.

Unclassified-Unlimited: Approved for public release.

Unclassified-Limited: Information exempt from public release by the Freedom of Information Act or other statutory authority. **Figure 1 gives examples.**

A DoD directive issued in 1970 established distribution limitations on technical reports which used the term. Unclassified Unlimited applied to information which was approved for public release by competent authority--an individual or organization authorized to release the information to the public, whether foreign or domestic.

Unclassified Limited meant that some official reason supported withholding information in technical reports from public release without approval by appropriate authority. The directive also provided reasons why a report should not be released to the public except upon approval by the contracting agency. The current directive that governs distribution limitation for technical reports is DoD 5230.24, Distribution Statements on Technical Documents.

Freedom of Information Act (5 USC 552) (b)

(b) This section does not apply to matters that are -

(1) specifically required by Executive Order to be kept secret in the interest of the national defense or foreign policy;

(2) related solely to the internal personnel rules and practices of an agency;

(3) specifically exempted from disclosure by stature;

(4) trade secrets and commercial of financial information obtained from a person and privileged or confidential;

(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(7) investigatory files compiled for law enforcement purposes except to the extent available by law to a party other than the agency;

(8) contained in or related to examination, operating, or conditional reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions;

(9) geological or geophysical information and data, including maps, concerning wells.

(c) This section does not authorize withholding of information or limit the availability of records to the public except as specifically stated in the section. This section is not authority to withhold information from Congress.

Figure 2

Many people overlooked a caveat in the 1970 directive warning against applying distribution statements on technical reports resulting from technical work on approved and funded technical intelligence, cryptology, communications security, and logistics documents.

The 1987 edition of the DoD directive broadens the areas of limitation and applies to "newly created technical documents generated by all DoD-funded research, development, test and evaluation programs".

As previously, the recent edition avoids applying distribution statements to documents containing cryptographic and communications security, electronic intelligence, and so on.

Freedom of Information Act (FOIA) Limitations

Almost everyone in this country knows about the FOIA as one of the most common reasons for limiting access to unclassified official information. Whether or not one agrees with the Act, it is the law of the land. It has been amended over the years as justifications for new exemptions were accepted.

Today, the problems we face in controlling Unclassified-Limited information are enormous. This state of affairs exists because declassification efforts have not kept pace with public pressures to declassify more information, and because the Government has failed to take the next step in reviewing unclassified information for public release.

Many legislative or regulatory authorities exist restricting dissemination of unclassified information. **Figure 2** displays a number of the well known exemptions from public release, and the basis for them. While the list is not exhaustive, it does suggest the desire to prevent public access to certain unclassified official information.

Complications Deriving from Global International Business

There are hundreds of international agreements that involve the exchange of unclassified official U.S. information: Government to Government, Government to Government with industry participation, and industry to industry agreements.

Most security specialists are acquainted with the North Atlantic Treaty Organization and agreements among its 16 members to protect classified information. Additionally, the Coordinating

Committee for Multi-lateral Export Control (COCOM), Australian Group, and Missile Technology Regime illustrate U.S. Government commitments with foreign governments to control certain unclassified information.

Not all such agreements take the form of treaties. There are also memoranda of understanding (MOU) with other governments, with and without industry participation; MOUs between the U.S. Government and foreign companies; and bilateral and multilateral ventures with foreign governments.

Industry, whether defense or commercial, or both, is global. That is a fact. Furthermore, such interaction with foreign entities has grown rapidly and is expected to continue to grow. The U.S. does not dominate unclassified (or classified) technology. In fact, it is fair to conclude that the U.S. is not capable of dominating the world technologically.

If we look at Operation Desert Shield/Storm as the most recent example, we see a multinational force that worked together, fought together, and operated together. Its national components communicated with each other, conducted a combined command and control system, and operated a common identification friend or foe warning system. They did this on land, on the sea, and in the air. That is the wave of the future.

Future operations will be combined operations, conducted with other nations regardless of whether the U.S. is the lead nation. Let us also remember that in Operation Desert Shield/Storm the U.S. citizen military reserve forces played a critical assistance role, which I will discuss later.

There is also a popular misconception that memoranda of understanding/agreement (MOUs/MOAs) cause the loss of technology. This is simply not true. MOUs contain provisions for the protection of classified and unclassified information, trade secrets, proprietary information, and bid packages. I quote from a recent report by the General Accounting Office:

> Since the mid-1980s, COCOM has acted to strengthen export control enforcement by (1) developing a common standard of enforcement that established several criteria (e.g., an effective legal basis, pre-licensing, and post-shipment checks) for COCOM members to meet; (2) encouraging non-members to adopt COCOM-compatible controls; and (3) requiring former Soviet allies to establish safeguard systems over COCOM-origin items.
>
> A key COCOM enforcement initiative has been the actions to develop a common standard of enforcement by COCOM members.

Because of its concern about the problems of fairness in defense, the NATO partners are considering a NATO code of conduct in defense trade which sets out a moral and political, rather than a legally binding, commitment by members of the alliance to improve the fundamental conditions of defense trade.

There is a need for a coherent U.S. policy on exports. A statement by the Director, International Trade and Finance Issues of the General Accounting Office observed that:

> Most industrialized nations have promotions to help companies sell products abroad. Collectively referred to as `export promotion' to include business counseling training, market research information, trade missions, fairs, and export financing assistance. Export promotion programs can play a useful role in increasing the export of a country's goods and services.

Only recently has the U.S. State Department issued a directive to its foreign missions to encourage and assist U.S. businesses.

Here we are, U.S. industry is falling behind in its ability to be competitive in many areas of technology. Foreign involvement is vitally important. Foreign companies are not always the bad guys. They provide many of the items needed to remain productive. Remember that we can no longer dominate technology.

It is fair to say that the U.S. has dominated military technology from World War II up to the recent past. But the U.S. has depended on foreign participation in armaments throughout our history, and today that is true more than ever before. So we must accept the fact of foreign participation in armaments.

It is equally fair to say that foreign components exist in practically all our major weapons systems. This is true in much the same way as foreign components exist in U.S. automobiles. Regardless of what politicians or car makers may say, there is no such thing as a purely U.S. automobile. **Figure 3** shows other recent examples of U.S.-foreign collaboration.

Examples of Recent U.S. Foreign Collaboration

1. U.S. Air Force to Examine Feasibility of F-22 Exports (Defense News, June 22-28, 1992)
2. G.E.-Led Consortium Torpedo Study-U.S.-UK Ship Torpedo Defense Project (Defense News, June 8-14)
3. U.S. Cuts Spur Sonobuoy Firms to look Overseas (Defense News, June 8-14)
4. ITT, Harris Join BAe to Bid for Bowman (Battlefield Radios) (Defense News, May 18-24)
5. U.S., Germany want Ex-Soviet Nations in COCOM (W.P. , May 31, 1992)
6. United Technologies, Siemans Reach pact (Defense News, March 30-April 5,1992)
7. LTV Aerospace, Inversa (Spain) Reach Pact (Defense News, March 30-April 5, 1992)
8. Lucas Aerospace (UK) GE, Ink Pact for Huey Gearboxes (Defense News, March 16, 1992)
9. When Corporate Lab goes to Japan (Eastern Kodak to Japan) to Conduct Research in Japan and Transfer Method to U.S. (NY Times, April 28, 1991)
10. Technology Forecast Post 2000 System Concepts, R&D Programmes and Key Technologies for the Security of Europe in the Coming Decades (NIAG - D (92) 1, Feb 1992)
11. Navy Hopes to Sell Europeans on Worldwide ASW Plan (Defense News, June 24, 1991)
12. Fujitsu Takes 44 PCT in Silicon Valley Company (W.P., August 29, 1991)

Figure 3

We Will Need to Exchange Information in the Future

The U.S. economy depends on foreign investment to operate. Much of the U.S. deficit is the result of borrowing from foreign investors. U.S. business depends on foreign banks for working capital, a fact that the DoD and the Defense Investigative Service have only recently become aware of. The U.S. dollar is cheap, and U.S. labor rates are among the lowest in the industrial world.

Why should foreigners steal U.S. technology? True, some countries are making the effort. But the industrialized nations are not the primary culprits. It is primarily third world countries that want and need U.S. technology--Saddam Hussein being a notorious case in point. It must be said, however, that many of the U.S. technology transfers were legal. The industrialized countries compete among themselves, and will go pretty far to get a sale, as "Ill-Wind" demonstrated. Finding out the plans, programs, and cost factors of competitors is merely good business. The U.S. is not without sin. We do, however, draw the line at bribes, as many malefactors have learned the hard way.

Why should foreigners steal from the U.S., when we do not lead in developing technology, especially when one looks at the rating sheets for critical technologies? Obviously, there are areas where the U.S. is ahead, such as software development and basic and applied research. But we do not lead in robotics, even though the principles were developed in this country. We do not lead in quality control, even though quality control principles originally were developed in the U.S. We do not lead in manufacturing technology. Unfortunately, we develop but we fail to fund long term investment in new ideas.

The point is, we are the idea people, the intellectual entrepreneurs, but we do not back risky development. And we even shun the vast amount of Japanese technology that is available. A National Security Council director for Asian affairs said recently that "the U.S. has not been active in pursuing Japanese technologies." Are we seeing an epidemic of the N.I.H. (not invented here) syndrome?

Up to now, our universities have been the best. But how long will that continue when our primary and secondary schools are in their current condition.

Can and Should Technology be Controlled?

Frankly, I take a simplistic approach to control. If research, regardless of the type, is bought and paid for, the payer has the right to control distribution of the results. Therefore, distribution can be controlled by the owner of the information. Note that I am not talking about shared ownership, patents, or licensing here; that is another issue that deserves to be addressed separately.

The issue is whether it is worth the time, money, and effort to control research for a given technology. Thus, the questions to be answered include the following:

* Are the results worth efforts to control?

* If importance cannot be assessed, should the information be placed in the archives to await future development, or should the information be made freely available?

* Do we have the technology today or in the near future to exploit the information, or do we want to push technology development so that the information can be useful?

* For industry, is there a potential market for the information, or is the information of such importance that it should be exploited and a market developed?

* If the information should be controlled, how long should it be kept under control?

What I am proposing is that, at a critical point in a project, we make an assessment to determine project effectiveness.

Obviously, every scientific and technical discipline is different. However, all must be examined critically at pre-determined check points. After all, projects must be funded; research and development is expensive; and money does not yet grow on trees.

The Threat -- A Personal View

Having been involved in the technical assessment on a world-wide basis for many years, and having been an active participant in the development of many of the control programs that are now in effect, I feel qualified to pontificate:

"YOU ARE THE THREAT!"

Yes, you. You are developers and implementers of policy, such as it is. But what have you done? Do you know the effects of your orders? Do you know what is going on at the next desk, the next office, or the other offices in your organization involved in the technical information process? Do you assume that if it is unclassified it is unimportant?

Do you know the laws on the books and the relation of those laws to your work? Can you make a judgement whether there is a justification to approve or deny a license application? Or whether to classify or not classify information? And do you know or are you aware of which company is doing what? Whether the end-user of the information is a good guy or a bad guy?

Here is an example from the public domain: The developer of the Iraqi long range rifle, parts of which were made in the U.K., was one Dr. Bull, an artillery specialist, a U.S. Government employee, who in the 1960s was working in a program with Canada to use a 16 inch rifle as a satellite launch vehicle. And this was long before he proposed a long range rifle to the Iraqis.

Unclassified information is your most important product. If it is worthwhile to fund a program, the results should be protected for as long as it is economically practical and feasible.

There are many impractical and unrealistic regulations and laws in effect to control information. And there is little real oversight. Unclassified technical information is the most critical. However, there is so much confusion on the issue that there have been few efforts to bring the subject under control. And there is still too much information that is classified, and the costs of protecting it are horrendous.

If you will examine carefully the list of existing directives, you will note that there is little effort to control basic research and applied research, whether in universities or in Government laboratories. Apparently, little effort has been made to establish a review mechanism, even though the research has been funded for a military purpose. After all, prior review is a "grievous sin." On the other hand, there is the example of total control, which generally does not work, either.

You will note that I have not discussed the differences between "secrecy" and "privacy" because they are difficult and contentious subjects unto themselves. Nor have I discussed "patents" and "patent secrecy," other subjects covered under Title 37, Code of Federal Regulations which need attention.

For you, the days ahead will not be easy. You will be faced with enormous demands from industry and the public to downgrade, declassify, and release to the public the mountains of classified information originated by the Government and contractors which has been ignored for many years.

I offer these points as guidelines for your deliberations:

> * Compliance with the existing regulations will help. It would be wise, however, to resist strongly all pressures for bulk release of documents to the public.
>
> * Remember, Unclassified does not mean publicly releasable.
>
> * There will be pressures to remove technical information from "Black" programs, Special Access Programs. As an aside, I would like to see controls reestablished that existed in Executive Order 12065.
>
> * You may be faced with doing the same or more with fewer people. in the past, the Army and the Navy have used their Reserve Components effectively for review and release.

In the final analysis, however, international cooperation is a fact of life, a fact that will continue to grow as far as we can see in the future. Donald Atwood, Deputy Secretary of Defense, made this clear in a speech in January 1992:

> By sharing cost and technology, and targeting programs at a much larger procurement need, we literally are ahead on all three counts.
>
> Such joint programs will be more necessary in the future--and acceptable to the United States--because it saves money, it provides standardization, and it does not take jobs away from us because we have a base that is much broader than just this country.
>
> Such a push is a high priority with me,and with Don Yockey, the Pentagon acquisition chief.
>
> Joint programs will not be limited to NATO partners; there is a good chance many such efforts could be undertaken with our allies in the Far East.

Note also that joint programs will not be limited to NATO partners, but will be extended to U.S. allies in East Asia, and perhaps elsewhere.

Figure 4 summarizes international cooperative activities that have expanded greatly in the past, and will continue to grow.

Summary of International Cooperation Activities

- o Cooperative R&D Programs: over 150 with 16 countries
- o Data Exchange agreements: over 750 with 25 countries
- o Engineer and Scientist exchange: 70 people with 14 countries
- o Co-Production Programs: 51 with 17 countries
- o Armament Cooperation Memoranda of Understanding with 21 countries
- o Defense Industrial Cooperation Memoranda of Understanding with three countries
- o Acquisition and Cross-Servicing Agreements with 17 countries
- o Logistics Support Memoranda of Understanding with Nine countries
- o Bilateral Meetings every 12-18 months with 22 countries

Figure 4

You must face the security challenge that international cooperation presents. You have the means, but need the will. There are enough laws and regulations now in effect. Enforce them, or cancel them. You must be able to make clear, rational decisions based on fact, not myth. Base your decisions on a knowledge of what is important and why, of where the U.S.fits in each technical and manufacturing discipline. Remember also that companies must know in detail why an export is denied. Pious statements such as "Trust us, because we cannot tell you" will not suffice. They simply will not fly. There must be valid, provable reasons why dissemination is denied. And you must know what should be protected, why it should be protected, the level of protection, how to protect it, and for how long.

My greatest gripe is that the Government does not comply with its own rules. There is no information security program that works. Government personnel are the principal violators of security regulations, and have done the most damage to the national security. Government personnel have committed most of the crimes. Government operates a two-track regulatory system:

"Do as I Say, Not What I Do"

There must be greater cooperation between Government and industry for the national good. No longer can it remain "Us" versus "Them." Unlike the old days, Government can no longer by itself build a ship, tank, airplane, or other platform. It must and does depend on industry. And Government must wake up to the face that this partnership, so called, is more like 51-49 and not 80-20.

On the other hand, industry must accept the fact that Government is the classifier. The intelligence producer must, under our laws, be number one. Like the old adage about the "Golden Rule," he who controls the purse controls the action.

I want to end on an optimistic note:

* The Commerce Department is doing a valiant job in helping our allies establish export control systems where they do not exist or are not adequate.

* In the not-too-distant future, there may well be common information and industrial security, contracting, and communications systems. The DoD and the Defense Investigative Service are trying to make this happen.

* There seems to be a greater feeling of responsibility among our allies to the dangers of terrorism. How easy it is to make an atomic bomb?

* The greater need for collective security is being recognized.

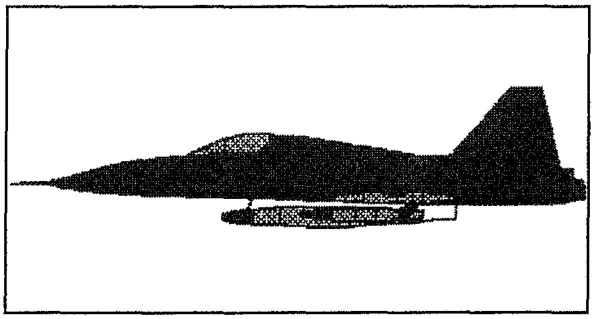
* Countries such as Sweden, which have historically been neutral, are seeing the need for military security and cooperation and have reversed their traditional aloofness.

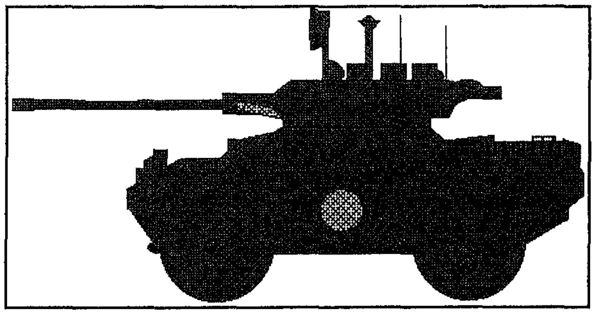
* Japan, with some trepidation, has passed a law which permits the use of the Japan Defense Forces outside the nation. It is interesting to note that a former member of the Japanese government recently proposed a conference on security and cooperation in Asia, with countries it overran in World War II.

* It is equally interesting that some of those countries have defense and industrial security agreements with the U.S. DoD.

So, this is the end of my sermon. I would be delighted to hear contrary views, and to be proven wrong on any point.

James J. Bagley is one of the NCMS founders. He retired from the Navy and now is President of R.B. Associates.





AIM HIGH AND BE ALL YOU CAN BE: ACHIEVING EXCELLENCE IN YOUR SECURITY PROGRAM

John P. Waller

Introduction

What makes an effective security program? Why is one company program extremely effective and another less than impressive? How does one security manager gain a sincere commitment to security from employees and another must wage a continuous battle to obtain support for the security program?

Granted, there are often uncontrollable constraints that can impact on the extent of success. Nevertheless, the overall success of a security program is directly proportional to the initiative of the security manager. He or she can take proactive measures which contribute to its success. Here are several of them.

Know the Regulations

By definition, the seurity manager is expected to be a subject matter expert. This does not mean that you must memorize the Industrial Security Manual (ISM), but it does mean that you should be familiar enough with the ISM that you can expeditiously find the section that provides guidance on a particular issue. Sometimes the governing regulation may be a security classification guide or amplifying remarks in a contract Form DD 254, or an Industrial Security Letter. For your program to be effective, you must thoroughly read these documents when they arrive and be familiar with their contents. The integrity of your program will be affected by the extent of your knowledge. If the engineers and scientists perceive that you are an expert, they will more readily listen and abide by your security guidance and direction.

Strive to Make Your Staff as Smart as You are (if Not Smarter)

How do you do this? The best way I know is by delegating responsibilities to your staff. When they must solve the problem themselves, they grow professionally, gain confidence, and many times will teach you things you did not know. My staff continually amazes me with what they are capable of accomplishing. By delegating and cross-training, you are able to effectively address security concerns even when one of the staff is absent. Strive to have no superstars on your security staff, including yourself. Your program will be stronger for it, and you will be able to take a vacation without the place falling apart while you are gone.

Keep Management Informed of Your Activities

By informing management of your efforts, they will appreciate your concerns and your contributions to the success of the corporate mission, and will ensure that security needs are addressed in the corporate budget process. Our CEO has a staff meeting every Monday morning at which the security manager is present to advise the senior staff on current security issues. This ensures that the security program is factored into weekly activities and keeps the senior corporate staff informed of our efforts.

Spend Time and Money for Training

Those with myopic vision will argue that money and time spent for training could be better spent elsewhere. However, the judicious investment in training for you and especially for your staff will result in time and perhaps substantial money savings in the future. An enormous amount of capital continues to be wasted on unnecessary security measures instituted unwisely as a result of ignorance of the regulations. When times get busy, the first casualty is often training. Insist on the continuance of external training (courses, seminars) and regular internal training (briefings, reviews of security regulations) for your staff, and of course, an effective security and awareness training program for the engineers and scientists. When time and money are scarce, a little creativity can keep the training program healthy.

Maintain the Integrity of Your Program

It only takes one incident to destroy the effectiveness of an entire security program. If one employee is treated differently from any other and it becomes public knowledge, the security staff will have an almost impossible task of effectively enforcing the security regulations in the next incident. Never compromise your integrity, and apply the security policy equitably across the board, regardless of whether the culprit is the new secretary, your assistant, yourself, or the Chief Executive Officer. If you are not prepared to do this, you might as well resign your responsibilities now. Let your staff know that maintaining the integrity of the security program is paramount and that there will be zero tolerance for inequitable application of the regulations.

Strive to Find Innovative Solutions to Security Challenges

Although your job is to say no when that is the appropriate answer, always qualify your no answers with "But let's see how it can be done within the regulations." It is easy to sit in your office and say no whenever something different arises. A professional security official will help the engineers and scientists accomplish their tasks effectively within the regulations. By discovering how the mountain can be gotten around, while still meeting the letter and intent of the regulations, you are telling them that you care about their needs. A good rapport with the technical personel will result. This rapport will translate into compliance and support for your program.

Know Your Company's Technical Mission

If you understand the technical aspects of the tasks to be accomplished by the engineers and scientists, you will better understand what is sensitive and needs security protection. Knowing what is being designed and developed, the objectives and procedures of test plans, the operational application of the equipment being built, travel requirements for test and evaluation, and particulars of equipment shipments will enable you and your staff to tailor a more effective security plan to the particular problem at hand. A good understanding of your company's technology is essential to proper classification management.

Understand the Technology of Your Security Equipment, Especially AIS

A modern security program incorporates many high-technology components. To be most effective, the security manager must understand their contributions to security. Know how your intrusion detection system works, and its capabilities and limitations; understand the technology of card readers; know how the classified document control software works; understand the vulnerabilities of STU III/secure facsimile operations; know the dangers of latent images on copiers and laser printers; understand how write-protection works on disks and cartridges; and understand the security capabilities and vulnerabilities of your AIS operating system. Understand how the local area network works, and which terminals and PCs are connected to the LAN; know about viruses and how they proliferate and how to protect your system from being infected. Know the difference between executable files and data files. Know the difference between volatile RAM, ROM, and long-term memory. Understand DOS, VMS, UNIX, and the capabilities of tools such as Norton Utilities. Do not be afraid of the technology. If you do not already know, ask the experts to teach you the basics. Ask the dumb questions. You do not have to become an expert, but consult with the corporate experts so that you have a basic understanding of the technology. You can enhance your knowledge by going to classes in the evening or reading tutorial books and technical magazines.

Associate with Other Security Professionals

When you attend professional meetings, such as the National Classification Management Society (NCMS), you can converse with other security professionals who will be able to share lessons learned not found in any book or article. We have learned of many innovative ideas at NCMS meetings that were later applied to our corporate security program.

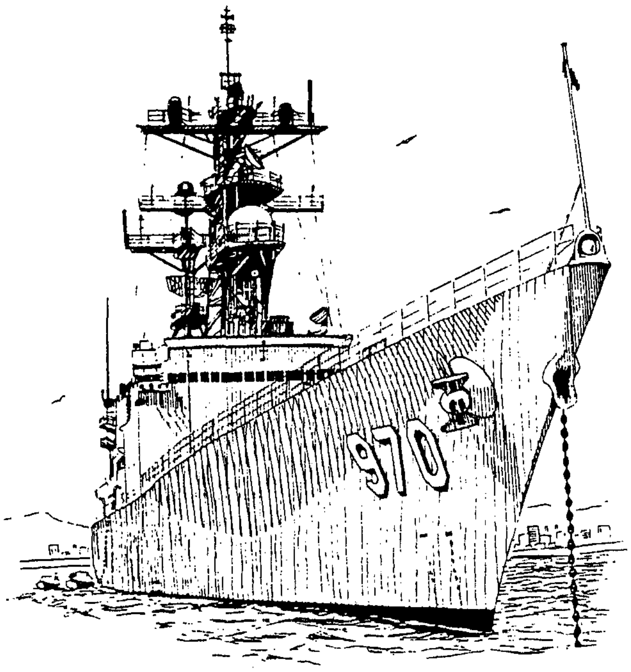
Read Security Periodicals

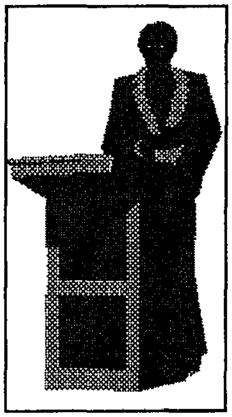
These may include NCMS Bulletins, Viewpoints, security magazines, ISLs, "News You Can Use," or a myriad of other periodicals that contain articles on security. Your security education is never completed. You must continue to read if you are to keep up with the changing security world.

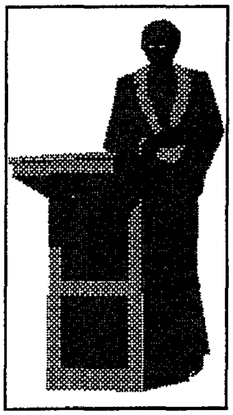
To have a strong security program, you have to pursue excellence actively. Your security program will not run effectively on remote control. Inaction and lack of initiative will result in mediocrity and eventually in a breakdown of security. The success of your program is limited only by your creativity, energy, and initiative. Strive to achieve excellence in your program and the sense of pride and achievement will make your efforts worthwhile.

After all, it's not just a job -- it's an adventure!

John P. Waller is security manager for the Syracuse Research Corporation in Syracuse, NY, and chairperson for the Mark Twain Chapter of NCMS.







THE NEXT THREAT:

Foreign Nationals in our Research Laboratories

Richard A. Black

National intelligence and security organizations have changed their focus. During the Cold War, and the hot ones, the "threat" was readily identifiable: The Red Menace. the Evil Empire. The Soviet Bloc. The Hostile Intelligence Service. It was relatively easy to postulate a threat and develop countermeasures.

In today's rapidly changing political and economic environment, however, we are told that "hostile" has become "foreign" and the objective is our technology, not necessarily our defense secrets. The war has become economic. In this new environment, friend and foe may be the same. Developing scenarios and countermeasures for external approaches is not a difficult task. I mean, what's the difference whether the external threat is Ivan the Terrible, Pierre the Perilous, Isahiko the Inscrutable, or Heinrich the Heinous?

"Friend and foe may be the same"

There is a potential threat which has far-reaching implications. It is our potential failure to recognize the diminishing availability of U.S. citizen research engineers and scientists. U.S. graduate schools in sciences and engineering are creating a virtual generation of foreign national PhDs. The former Soviet Union, East Bloc countries, People's Republic of China, and others are producing leaders in many technologies of vital interest to the U.S., many of them through our academic institutions.

An editorial in the San Francisco Chronicle on 2 February 1988 states "A panel of the National Academy of Engineering has reported that in 1985 45 percent of engineering graduate students at all levels were foreigners living in this country on temporary visas, and another 10 percent were non-citizens with permanent resident visas." This situation has not improved. The questions we must ask ourselves are "What will be the impact on advanced technology research and development in the late 20th and 21st centuries? " and" What is our ability to protect our nation's vital technologies?"

The contributions made to the present state of U.S. technology by such individuals as Werner Von Braun, Edward Teller, and many others is fully recognized. When it has been clearly in our national interest, clearances and required accesses have been granted. Given that the finest minds and technical qualifications needed by industry today may belong to foreign nationals, will it be in our national interest to do so again? I believe the obvious answer is yes. Over 1400 Limited Access Authorizations have been granted to permit foreign nationals access to defense classified information. Requiring U.S. citizenship for performance on classified contracts will not be an acceptable solution if we are to maintain our technology leadership position in the world.

President Bush's call to improve our educational system, particularly as it relates to mathematics, engineering, and science instruction, will not be evident in industry for at least 20 years if we start now. And that's only if we are successful in convincing today's first grader to concentrate in these disciplines. Thus, the dwindling pool of U.S. human resources creates the likelihood of increased foreign national presence in U.S. research and development facilities.

So what is the impact? Under these circumstances, in addition to the classified access problem, the control of unclassified technology transfer will become an even greater challenge than it already is. There is not the relatively clear guidance offered by the Industrial Security Manual, and hopefully the new National Industrial Security Program Operating Manual, now in draft form. This is because responsibility for technology protection falls in at least two, and as many as 12, different government agencies depending on the nature of the technology involved. In some cases, the Department of Defense will be involved, even though the technology in question is unclassified. Remember Unclassified, National Security Related Information?

One of the problems for the industrial security manager is that, by definition, a verbal exchange between a U.S. national and a foreign national constitutes an export. Therefore, for this verbal exchange to occur properly, an Export License must be in place. Then, the U.S. national has to know what can be said and what cannot. Realistically, how can the dialog between colleagues working in the same technology be monitored? What do you do when the senior manager of the lab, center, group, or division responsible for the technology is a foreign national?

It is also important to remember that unclassified technology disclosure need not be intentional to qualify for civil and criminal penalties. Frankly, this should concern us at least as much as, if not more than, the inadvertent disclosure of defense classified data. In most instances, although gross negligence can lead to revocation of the Facility Security Clearance, when a security violation involving defense classified material occurs, an investigation is conducted, procedures modified, personnel reprimanded and retrained, and agreement is reached with the Government, after which it is pretty much business as usual. With technology data transfer, punishment can be swift and harsh.

One simple answer is physically to separate U.S. and foreign national employees. In the real world, however, duplication of research facilities is terribly expensive and normally not feasible. Furthermore, the development of technology breakthroughs requires the relatively free exchange of data and ideas by colleagues working the problem. Note the verbal exchange problem addressed above.

Another simple answer is to use the existing Limited Access Authorization (LAA) program. The increased administrative requirements for industry and Government could become a nightmare. In these times when overhead dollars are tight, in some cases non-existent, waiting for an LAA or approval from a contracting office could result in significant expense for an employee. Not hiring these highly qualified people is not an answer in times when competition is won by the company with the latest technology at reasonable cost. No one can afford to be second best, especially our nation. It is in our national interest to take advantage of the brightest and best minds, regardless of what nationality is represented. So, the Government must develop a sensible policy to deal with access to classified information by foreign nationals. The present LAA process is not it.

"Government must develop a sensible policy to deal with access to classified information by foreign nationals."

So much for the easy part. How do we develop this policy while protecting our sensitive technologies? First, it is essential that the U.S. Government develop and implement a standardized national technology security policy. This policy would establish not only what controls are essential but also identify those technologies our Government has determined to be vital to our national interests. This process necessarily must include industry. Perhaps we need more, not fewer, Special Access Programs. This last statement may be judged pure heresy coming from a security professional who has spent considerable energy over the last 15 years remonstrating against the proliferation of unnecessary caveats and increased security requirements. Note however, that not all technologies need this level of protection.

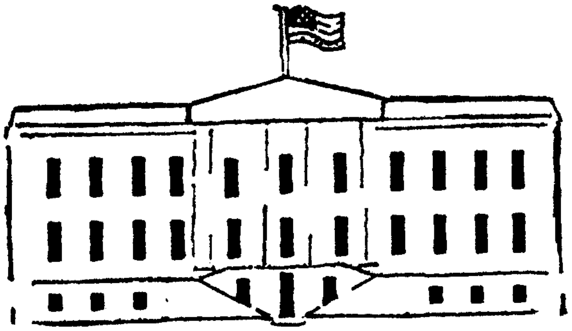
The generic development of a technology, for instance, could be done totally open while the specific application of the technology could be totally hidden. This would permit development of the generic technology by qualified engineers and scientists regardless of citizenship, while the application, a small part of the whole, could be protected and performed by a limited number of U.S., and even foreign, nationals.

This approach seems reasonable given today's direction for the dual use and commercialization of technologies. No longer can industry afford to have the Government as its only client. No longer can developed technology be withheld from commercialization, even exportation. And no longer can Government afford to fund all basic research and development. But we must maintain, even increase, our technology development. Unless we address the issue of the growing number of foreign national scientists and engineers in our leading research facilities, that possibility is in jeopardy.

"We must maintain, even increase, our technology development."

There is presently discussion regarding establishment of a national technology evaluation organization. Consideration is being given to have the organization under Department of Defense management. In the national interest, it would be far better to have some other department manage it. The narrow perspective of DoD would ultimately lead to limited commercialization and exportation of technology because a case can be made that virtually every technology has dual use possibilities. Leadership of this new organization must take a longer view advocating improvement of the national economy, and accepting a broader risk by permitting expansion of U.S. business through exportation. Inevitably, this will involve using available foreign national human resources with the skill and knowledge to create new technology.

Richard A. Black is director of security education and training for SWL, Inc., a wholly owned subsidiary of GRC International in Vienna, VA. He most recently served as director of corporate security for SRI International in Menlo Park, CA. In the latter capacity, he won the Cogswell Award for excellence in industrial security.



NATIONAL SECURITY CLASSIFIED INFORMATION IN THE PAPERS OF FORMER GOVERNMENT OFFICIALS

Jeanne Schauble

For many years, historical societies and university libraries have actively solicited the personal papers of prominent individuals in order to preserve them and make them available for historical research. Such collections are indispensable sources of information for historians. Former Government officials, especially cabinet level officials and former Senators and Representatives, are favored targets for such solicitations. These same former officials are aware of the value of preserving the historical record and usually respond positively to requests to donate their papers. Many officials consciously collect duplicates of official papers and other records of their Government service with the thought of writing their memoirs and donating the papers to a historical institution. Information security managers are frequently surprised to discover that these donated personal papers include classified information. How does this come about?

The practice of Federal officials removing their papers when they left office goes back to the earliest days of the Republic. George Washington, concerned that no official provision had been made for the records of his Presidency, packed the records into trunks and took them home to Mount Vernon. This precedent was followed by his successors and it became a tradition that the President's papers were his personal property to be disposed of as he wished at the close of his administration. Many of the records of the Presidency were lost, dispersed to collectors or destroyed accidentally or deliberately. Senators' and Representatives' office files are their personal property to do with as they please and have encountered fates similar to Presidential papers.

In the rest of the Government, although many agencies accumulated large quantities of records, there was a similar lack of consideration for the disposition of records once they were no longer needed for the conduct of current business. Departmental records were stored in attics, basements, and warehouses, often under less than ideal conditions. Many were lost to fire, flood, or other disaster. An 1810 Congressional investigation into the condition of the records of the Continental Congress led to the first attempt to provide space specifically for storing Government records. This and several succeeding attempts failed to arouse Congressional interest despite a number of fires in Government buildings that destroyed large quantities of valuable records. The idea of providing safe storage for Government records finally began to gain support in the late 19th century. However, it was not until 1934 that the National Archives was established to provide for systematic preservation of the permanently valuable records of the United States. In the meantime, many high level Government officials were following the example of the Presidents in treating their office files as personal papers.

President Franklin Roosevelt was concerned about the lack of provision for Presidential papers. In 1938 he proposed to build a building on his estate in Hyde park, New York, to house his personal papers. The building was to be built through private contributions and turned over, with the papers, to the Federal Government on completion. The Government would then maintain the building and eventually make the papers available for historical research. Subsequent Presidents (and one preceding president, Herbert Hoover) followed his precedent, resulting in the system of Presidential Libraries that is part of the National Archives system. The example set by Presidents further encouraged both the collection of personal papers by Government officials and their solicitation by historical institutions.

Another factor that used to encourage officials to collect and donate their papers was the tax deduction that could be taken. Donors of personal papers were allowed to deduct the assessed value of the papers as a charitable contribution. By the time this deduction was eliminated, most high level officials were routinely being solicited by one or even several institutions for the donation of their papers.

In recent years, officials have benefited from keeping collections of personal papers to assist in writing their memoirs. They may negotiate an agreement with a historical institution that allows them and/or a research assistant exclusive access to the papers while writing the memoirs, and sometimes office space and other assistance in return for donating the papers to the institution.

There are several reasons, then, why Government officials accumulate masses of personal papers, some of which may appear to be Federal records, including classified information. For many years, agencies did little to monitor the removal of personal papers by high level officials. Henry Morgenthau, Secretary of the Treasury under Franklin Roosevelt, removed much that should have remained as part of the official records of the Secretary of the Treasury. In fact, agencies sometimes cooperated with a cabinet officer's donation of papers to a private institution. The State Department, for example, microfilmed records, including many classified documents, for Secretary of State John Foster Dulles which he donated to Princeton University. These records are still classified.

One byproduct of the Watergate scandal that forced Richard Nixon from office was the focusing of attention on the status of Presidential papers. Following Nixon's resignation, Congress passed the Presidential Recordings and Materials Preservation Act which retained the official records of the Nixon Presidency for the Government. In 1978, Congress passed the Presidential Records Act declaring documentary materials created by the "President, his immediate staff or a unit or individual of the Executive Office of the President" which reflect the performance of his "constitutional, statutory, or other official or ceremonial duties" to be Presidential records. The act requires that Presidential records be filed separately from personal materials and that the records be placed in a "Presidential archival depository" under the control of the Archivist of the United States when the President leaves office. (However, the Act specifically allows the records of the Vice President to be placed in a non-Federal archival depository when the Archivist determines it to be in the public interest).

The changes at the Presidential level have led to increased scrutiny of departing officials at the agency level to ensure that they are not leaving with official records. Congress has also established policies concerning the removal of classified information with a departing Senator's or Representative's papers. Why does classified information in private papers continue to be a problem?

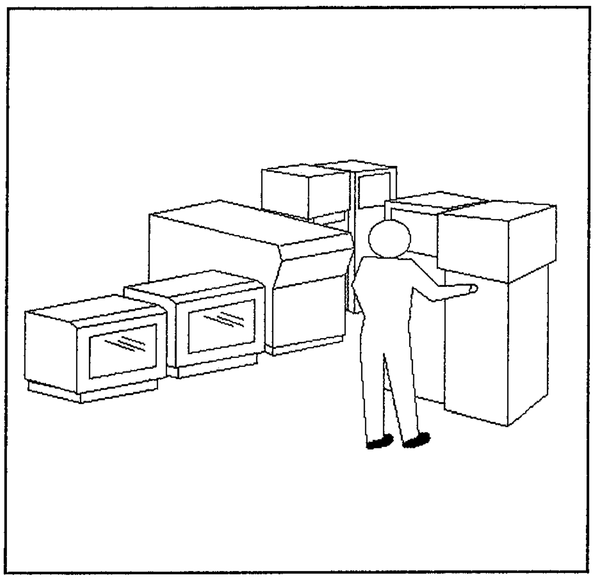
In some cases it is merely an instance of an old problem just coming to light. Government officials or their heirs may wait many years before donating papers to a historical institution. In other cases, the institution may have realized at the time of receiving a donation that the classified information could not be released and is only now seeking assistance in making it available. Or the institution may only now be archivally processing an older donation and discovering that it contains classified information.

In some cases poor filing practices led to the intermingling of official and personal papers resulting in the unwitting removal of classified documents. Agency processing-out procedures for departing officials are designed to ensure that the officials do not remove Government records. The record copy of a document is the original or official file copy. Copies of Government records kept solely for personal or reference use are not official records and therefore may be taken by a departing official. Many officials who plan to write memoirs deliberately keep copies of the most important documents pertaining to their Government service, sometimes including copies of classified documents.

Classified information does continue to go out the door with Government officials, although not in the quantities that it once did. Agencies are making greater efforts to ensure that the security classified documents in an official's personal papers remain within Government control until they can be declassified. The National Archives has recently drafted an amendment to the Code of Federal Regulations that would require an official to obtain permission from the agency head before removing extra or personal copies of Federal records. The Archives has also published "Personal Papers of Executive Branch Officials: A Management Guide" which provides guidance to agencies and officials concerning the removal of personal copies of records, including security classified materials.

Ultimately, however, the agency and departing officials share the responsibility for preventing the loss of control of classified information. The agency must publish clear standards for distinguishing between agency records and personal materials and for what types of extra copies an official may consider to be part of his or her "personal" papers. The agency must also enforce these standards during the processing out of a departing official, even at the highest level. For his or her part, it is the responsibility of the individual official to identify any security classified documents he or she wishes to remove as personal papers and to consult with appropriate agency officials to make arrangements for declassification or storage of the papers in an approved facility.

Jeanne Schauble is Director of the Records Declassification Division of the National Archives of the United States.



SOLVING SECURE DATABASE CLASSIFICATION MANAGEMENT PROBLEMS

Gerald L. Kovacich

Introduction

In today's technological, knowledge-based environment, the use and size of automated information systems (AISs) are growing rapidly. They are used to facilitate the sharing of information among millions of users at hundreds of thousands of locations. Advancing technology makes it easier to provide more information to more people so "the world can talk to the world."

A secure environment where information is limited to those users who have a need-to-know presents a unique challenge to the security professional: How can information be protected and limited based on need-to-know when others are driving the technology to give more people the ability to share more information?

We are so used to dealing with computer systems that we believe more secure hardware and software can solve the security problems associated with computers. In some cases this may be true. Occasionally, however, we forget the basics of solving security problems and look to the computer as the panacea. It is not. It is only a tool that can sometimes be used to help solve security problems.

We must not forget the basics, the security methods and solutions developed and tested over the decades which work. Two such methods are classification management and the security requirements identification processes. They are still valid in the computer environment. We just need to update some of them and adapt them to the changing AIS environment.

Trusted Systems

The following discussion of Multilevel Secure (trusted) Database Management Systems (MLS/DBMS) is used to illustrate my point.

Trusted systems are those systems developed by computer companies which meet the standards set forth by the National Computer Security Center (NCSC). The baseline standard is the Department of Defense Trusted System Evaluation Criteria, CSC-STD-001-83 (the "Orange Book"), and is supplemented by related documents known as the "rainbow" series. These systems are submitted to NCSC where they are tested. Once approved, they are rated to provide a certain level of trust. The higher the criteria rating given a system, the higher the level of trust in the system to secure itself.

The Trusted Database Management System Interpretation of the Trusted Computer System Evaluation Criteria, (NCSC-TG-021, Version-1) dated April 1991, published by the National Computer Security Center, defines several key terms:

A. Database management system: A computer system whose main function is to facilitate the sharing of a common set of data among many different users. It may or may not maintain semantic relationships among data items.

B. Trusted Computing Base (TCB): The totality of protection mechanisms within a computer system including hardware, firmware, and software the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of a TCB to correctly enforce a security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e.g., a user's clearance) related to the security policy.

Based on the above and if everything works as designed, users cannot gain access to any information to which they have not been granted access. The question is, however, whether they can gain access to information for which they do not have a need-to-know by putting together that information which is unclassified and to which they have access, and/or being "told" by the system that they cannot have access to certain, specific pieces of classified information.

The Inference Problem

The answer to the above question is yes, through inference.

Inference is defined by The American Heritage Dictionary as deriving a conclusion from facts or premises. Infer is defined as concluding from evidence or premises or having as a logical consequence, or leading to as a consequence or conclusion.

It can be likened to a piece of a puzzle that is missing. Since other pieces which surround it are in place, you know the shape and size of the missing piece. Additionally, most likely the printed pattern, color, and texture of the missing piece can be determined by the pattern, color, and texture of the surrounding pieces. Although it is absent, you still know something about it. Since you have a pretty good idea of what it looks like, it will help you in your search for it.

This is the same basic method used in espionage. It is a continuous probing, gathering of bits and pieces of information, and fitting them together to form bigger pieces of the entire puzzle.

The inference problem in MLS/DBMS, at first glance, tends to lead one to believe that the solutions are to be found within the MLS/DBMS environment. Taking a more basic and systematic approach, however, would lead one to identify the root problem as one of an outdated process approach for a manual system which is being applied to a new automated environment.

Any attempt to solve the problem immediately through analysis of MLS/DBMS itself would only be treating the symptom, not the problem. The problem of inference has always been there on a smaller and more dispersed scale. It has recently been highlighted and compounded due to automation of databases, a massive amount of information concentrated in one fixed location available to many more people at a given time.

In the case of the inference problem, the processes involved in the classification of information and system security approval must be properly analyzed. Automation, the MLS/DBMS, has developed; however, the security processes associated with that type of environment have not been modernized to keep pace with the technology.

The manual process used to deal with such problems caused by automation, such as the inference problem, were based on hardcopy documents in a manual system. Compartmentation of information was as easy as physically separating the documents and program areas. Technological advances clearly have left security processes far behind. This has resulted in ever-increasing risks to national security information since modern, automated systems are being rapidly configured for total integration because of the drive to share information.

The inference problem may or may not be an issue which can be solved. If it is, it must be approached systematically. In doing so, it is necessary to begin at the beginning, the philosophies, methodologies, and processes utilized in determining not only what is classified, and processes utilized in determining not only what is classified, but also the basis for that determination.

Inference Example

The following example points to the problem that is primarily a non-automated problem. If the number of warheads on a missile were classified, but the member of bolts used to secure each warhead was not, nor the total number of bolts used to secure the warheads, it can easily be seen that, by dividing the total number of bolts by the total bolts per missile, the total number of missile warheads can be determined.

This example points to a type of problem which would exist regardless of the security level of the MLS/DBMS. Why? Because it is not an automation problem. It is a classification management problem first and a derivative MLS/DBMS problem, that is, an automation problem, by inference.

Thus, before looking for the solution in hardware, software, or other aspects of the automated system, first look at the manual process. It may provide the solution as a matter of approaching the classification management issue from a different process analysis viewpoint.

The Process Quality Improvement Approach

By using a process quality improvement (PQI) philosophy, this problem may be solvable. The four-step approach is to:

1. Understand the current process;
2. Document the current process;
3. Analyze the process; and
4. Change the process. Then, if feasible, automating the process can be considered. You will note that the use of automation is the last thing to be done. The obvious reason is that automating a process which has not been analyzed and simplified through PQI would compound the problems to such an extent that problems are more likely to be created. In this case, it may lead to information being more vulnerable to compromise.

By taking a process analysis approach instead of immediately looking at possible automated solutions, the solutions could be portable to any platform. With the trusted system approach, a company would be tied to a particular system through a sole-source vendor. The ramifications could be costly.

The Approach

To resolve the problem, we must look at the manual process, methodologies, and philosophies which have a direct bearing on the inference problem. It would not only provide the opportunity to help resolve the inference problem, but also assist in modernizing the classification management process itself. It could provide enhancements or even new philosophies and methodologies which will provide modern processes which can be integrated into today's and tomorrow's modern technology. It may even provide new ways of addressing other AIS security issues, thereby achieving more efficient quality processes which also minimize the risks of compromise of national security information.

To derive solutions to the inference

problems which occurs in the MLS/DBMS, the following approach should be considered:

1. Define the classification management process.

a. Obtain classification management policies, procedures, etc. from the customers.

b. Gain a basic understanding of the customer's unique processes.

c. Document the flow process and develop a flowchart of the customer's basic classification management process.

d. Analyze the process.

e. Identify portions of the process which may have a direct bearing on the inference problem in MLS/DBMS.

f. Simplify and recommend changes to the process to integrate into the automation environment.

2. Develop security classification guides.

a. Obtain security classification guides from the customers. Customers should provide a sampling of classification guides, any training material and associated documentation used by those who developed the guides, as well as policies and procedures which identify, establish, and explain how classification guides are to be developed.

b. Gain a basic understanding of the customer's unique processes:

(1) The documentation will be analyzed to determine its adequacy, consistency, and application across multiple programs where national security information is residing in a MLS/DBMS.

(2) A survey questionnaire will be developed and used to determine the methodologies used in the development of classification guides, the philosophies used, and so on.

(3) With customer's support, surveys will be conducted of personnel identified by the customer who have written the policies and procedures related to classification guides and other professional classification management personnel.

c. Document the flow process and develop a flowchart of the customer's basic classification process using PQI.

d. Analyze the process.

e. Simplify and recommend changes to the process to integrate into the automated environment.

f. Identify portions of the process which may have a direct bearing on the inference problem in MLS/DBMS.

3. Use artificial intelligence/expert systems (AI/ES).

Once the classification methodology has been analyzed, the use of AI/ES will be researched as possible analytical tools. Approaches to use AI/ES are as follows:

a. Analyze and document the AI/ES methodologies that may be applied to the classification management process. Research AI/ES techniques and identify those that may have applicability to the inference problem.

b. Analyze and document the AI/ES methodologies that may be applied to the security classification guide process. Develop methodologies using AI/ES which can be applied to the inference problem.

c. Establish AI/ES systems which may be used as tools.

4. Define security requirements and perform process analysis.

Assuming that the MLS and DBMS are installed and operating in accordance with their security-approved configuration and associated documentation, it may be that the security requirements and processes, as implemented and approved by the Government security personnel, are not conducive to actually providing the necessary protection required in the MLS/DBMS environment.

a. Obtain security requirement policies and procedures from the customers. Customers should provide a sampling of standard practice procedures (SPP), any training material, and associated documentation used by those who developed the SPP, as well as policies and procedures which identify, establish, and explain how the individual security documentation is to be developed, used, and updated.

b. Gain a basic understanding of the customer's unique processes

(1) The documentation will be analyzed to determine its adequacy, consistency, and application across multiple programs where national security information is residing in an MLS/DBMS.

(2) A survey questionnaire will be developed and used to determine the methodologies used in the development of SPPs, the philosophies used, and so on.

(3) With customer's support, surveys will be conducted of personnel identified by the customer who have written the policies and procedures, e.g., SPPs, and other professional Government and contractor personnel.

c. Document the flow process and develop a flowchart of the customer's basic security requirements and procedural approval processes using PQI.

d. Analyze the process.

e. Simplify and recommend changes to the process to integrate into the automation environment.

f. Identify portions of the process which may have a direct bearing on the inference problem in MLS/DBMS.

5. Identify possible solutions.

Based on the above, a set of recommended solutions to mitigate and/or resolve the inference problems in MLS/DBMS will be identified.

6. Implement a pilot prospect.

a. Develop scenarios and profiles of users to include:

(1) A normal user of the MLS/DBMS.

(2) A mole who will attempt to use the inference problem to gain access to unauthorized information, and

(3) A counter-mole to look for patterns and trends indicative of a user (mole) utilizing the methodologies developed.

b. Test, analyze, change the processes, and test again until the processes are fine-tuned to the maximum extent possible to protect the information requiring protection.

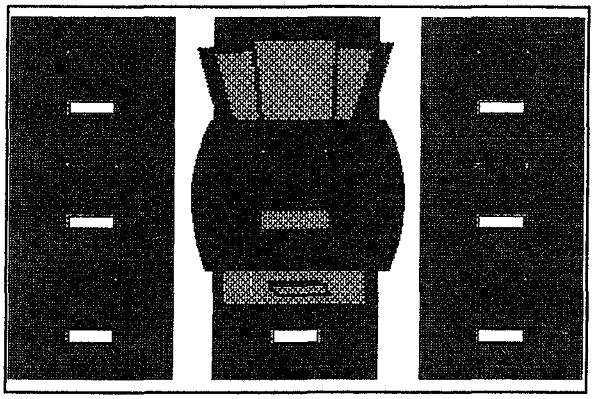
7. Document results and implement the new process improvements.

Summary

The trend to share information through the use of computing systems will continue to grow. The new security vulnerabilities associated with new technologies will also increase. The thrust of the protection of automated information based on a need-to-know is through trusted systems. Before looking to these "trusted" systems to solve computer-related vulnerabilities, let's look at updating and enhancing security methodologies and philosophies that have been tested over time and which work. The security basics still apply. Perhaps we just need to modernize and then apply them to the new environment. *

* This could be the basis of a project for NCMS and the U.S. Government to work together as a team.

Gerald L. Kovacich has 29 years of experience in Government and contractor security. He is currently the manager of investigations and security inspections for Northrop's B2 Division.



IS ACCOUNTABILITY OF SECRET MATERIAL LOGICAL?

Jeanne Bastoni

Technology in all fields of endeavor has progressed at such a rapid pace over the last twenty to thirty years that we are hard pressed to recognize all its ramifications. The proliferation of copiers, fax machines, and computers has enhanced the ability of the unscrupulous to convey classified information to hostile governments while rendering document accountability procedures useless.

The rules for accountability of classified material were instituted at a time when a missing document meant that it possibly was stolen for nefarious purposes. Today, it is highly unlikely that the individual who is intent on committing espionage would abscond with the original document. There are too many other more efficient means to divert the information. One might simply make a copy or fax the document to a confederate. Provided with a computer and a modem, the perpetrator could transmit classified data quite easily. One of the infamous Walker brothers took Confidential documents out at lunchtime to his van, where he copied them, and then returned them to a file upon his return to work. No one was the wiser.

These acts are committed by persons who have a clearance and easy access to classified information. They, of course, are the ones who usually are recruited, or volunteer, to provide classified information to foreign interests.

With these points in mind, we must now ask ourselves, what do we expect to learn through document accountability--that a classified document is missing from a file? Is it reasonable to assume it has been stolen? More likely, it has been misfiled, loaned to an authorized co-worker, sent to another (authorized) contractor facility, or destroyed. It is probable that as a result of a clerical error, the record does not reflect the current or correct status of the document.

One point in favor of document accountability is that it facilitates disposition or retention authorization of material when a contract ends. Of course, Confidential material must also be disposed of at the completion of a contract, and there is no accountability requirement for Confidential. We must rely on the custodians to identify the material received or generated under any given contract.

As for knowing what classified material is on hand at any given time, we can only estimate Confidential material; is it really less important than Secret? The Walker brother who copied the documents at lunchtime is spending the rest of his life in prison for stealing only Confidential material. And he was not apprehended by the discovery of a missing document in his file, nor were any of the others in this master spy ring.

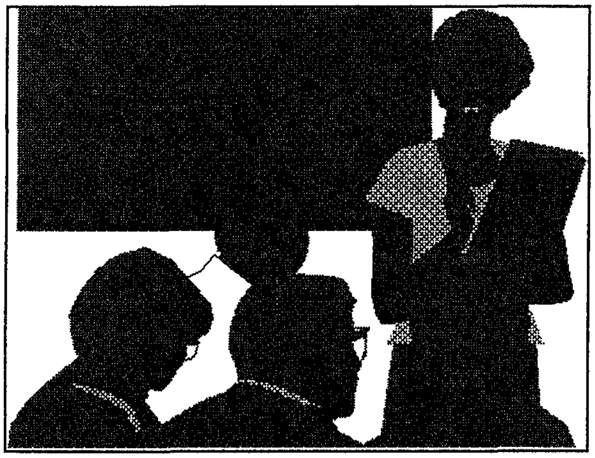
Perhaps keeping records of the receipt and dispatch of Secret material would be adequate, as is for Confidential. (Top Secret is not being addressed because there is so little of it compared to Confidential and Secret and it requires special handling.) Generation of Secret should also be recorded. Our time may be better spent in the actual safeguarding, marking, limiting access, and education of custodians.

To maintain tight accountability of all Secret material requires considerable time, effort, and money. To justify it, there must be a practical purpose served. Do we protect

Secret more carefully because the custodian is personally responsible? The penalties for mishandling Confidential are the same as for Secret.

Eliminating the requirement for strict accountability of Secret material is not to say we should in any way relax our procedures for protecting the information. If anything, we probably should increase our vigilance and controls. More emphasis should be concentrated on the individuals who handle classified material. It should be stressed that they have a legal as well as a moral obligation to safeguard the classified information with which they have been entrusted.

Jeanne Bastoni is Security Manager for Dynamics Research Corporation in Andover, MA.



TOTAL QUALITY SECURITY TRAINING:

A Blueprint for Training in the Nineties

Adam L. Gardner

What is total quality management (TQM)? How do you implement a TQM system for training in your organization? What are the benefits of TQM for training? Answers to these and related questions are developed in this article by applying the elements, principles, and promise of quality improvement training to security organizations.

The Training Challenge

What has been successful for dealing with our adversaries in the 1980s may no longer work as we push into the 1990s and beyond. We are beginning to recognize that we have to restructure our way of thinking and doing business concerning the protection of our classified and sensitive assets.

In order to meet this challenge, many organizations are undergoing a major overhaul. This trend is toward quality training-- identifying and meeting individual employee needs. Training will have become more dynamic to adapt to the new challenges.

Unfortunately, in this constantly changing world-wide security venue, "Loose Lips Sink Ships" just does not cut it anymore. As the need for quality-awareness increases, so will the demand for more fluid, just-in-time training models. These changes mean more precise and better articulated training.

Why Enhance Security Awareness?

The case for enhancing security awareness in Government and industry can be made by examining three areas of concern: the role of Federal Government in security training, the ingredients of a good security education program, and the potential for success through Total Quality security Training (TQsT).

Federal Government Role

The first area of concern addresses the Government's roles in security education and in security training, and how these differ. Enhancing security education and training has become a major concern for Government and industry alike, especially at this time when Europe and the former Soviet Union are redesigning maps. This is a time of discontinuity and disbelief, of uncertainly and ambivalence. As difficult as it is for some security trainers to find anything concrete to hang on to, we can only imagine what this new age must look like through the eyes of new security trainers who lack the expert knowledge and the resources that are well known to most professionals in the business,

It is important to establish clear-cut definitions of training, education, and awareness and to distinguish among the three. The terms are not interchangeable.

Training is narrow in scope and involves only learning that which is directly related to job performance, while education is thought of as being much broader in scope and is concerned with the total human being and that person's entire world. In practice, training and education frequently occur at the same time.

The common thread running through all three terms is change.

- Training is a change in skills (skills required for program implementation).

- Education is a change in knowledge (to demonstrate solid understanding of security policies, principles, and procedures).

- Awareness is a change in attitude or values (acknowledgement of the existence of the foreign economic and intelligence threat and understanding of foreign intelligence collection methodology).

Security Education Program Ingredients

The second area is based on Mr. Joseph A. Grau's talk titled "Security Education--Something To Think About" presented at the National Classification Management Society's Eighteenth Annual Seminar in May 1982. According to Mr. Grau, there are four basic components to a good security education program. All four must be present for your program to be effective and to satisfy the requirements of our various regulations and directives. These four components are:

- Awareness--acknowledging the existence of the foreign intelligence threat and understanding the foreign intelligence collection modus operandi.

- Motivation--engendering the desire to apply good security practices on and off duty.

- Education--knowledge of policies, procedures, and philosophies that make the skills necessary and meaningful.

- Training--skills needed for actual hands-on operation of specific security tasks.

TQsT

The third area of concern involves a new approach to training, one that is very powerful. TQsT extends beyond merely coping with traditional training problems and leads toward positive action.

Visions of TQsT

One of the great pioneers and innovators of the TQsT concept was Mr. Robert W. Wells, who retired as Deputy Director of the Information Security Oversight Office (ISOO) in January 1989 and died in September 1990.

In November 1987, he lectured on security education and training during the Intelligence Community Security Education Seminar conducted at the FBI Academy in Quantico, VA. He provided each seminar participant with a list of his twelve security training maxims that are as valid today as when first introduced. Eight of his twelve maxims reveal a vision of TQsT:

- It can be expected that most security managers and technicians will continue to be persons with little detailed experience or knowledge of security--their security functions will be additional duty assignments.

- Security is not and will never be a thrilling or tantalizing subject to teach or to be taught.

- With the rapid growth of technology, the tasks of security educators will become increasingly more complex and difficult.

- There will be an increased need for obtaining command and supervisory support and commitment to training efforts. That old adage "an organization does well those things the boss checks on" never was more appropriate.

- Security educators must be willing to devote more of their own time to becoming familiar with new techniques and procedures--they must keep up!

- Security managers and educators must strive to make security education and training more concise, more interesting, and to the point.

- Time, budget and personnel restraints will dictate that security manager and educators share as much as possible the many good training ideas and training aids already in existence.

- Increased efforts must be devoted to the development of security education material that will, as far as possible, be universal in its application to government and industry. Any new development should not be done in a vacuum; rather, security managers and educators must be aware of each others' efforts and must be afforded the opportunity to use the fruits of each other's efforts.

Unquestionably, the most significant by-product of these maxims are the formulation, testing, and dissemination of a systematic approach to the design, development, validation, and implementation of TQsT.

Introducing TQsT to your Organization

TQsT is a process that combines people, materials, methods, machines, and the environment in a way that adds value to a product or service. For example, the process of designing a training course requires making optimal use of the people involved; using the books and articles written on the topic; integrating the work of individuals and groups; computers and copiers; and the lighting, ventilation, and distractions in the work area.

Manufacturing considers inputs, processes, outputs, and customers. TQsT considers these as well. The input is your new employee or assignee. The process is the security orientation, indoctrination, or training course. The output is the indoctrinated employee, the employee with increased security awareness, or the graduate of a security training course. Our customer is the supervisor on the job.

As you might expect, TQsT in any organization can be viewed as a key quality control function, as shown in **Figure 1.** This diagram suggests that:

- The TQsT function is a process, converting training needs data, training technology, training expertise, budget, and untrained personnel into trained personnel for various operating units.

- The primary inputs of training needs and untrained personal are converted into the output of trained personnel through processes such as analysis, design, development, delivery, and education.

- The quality of the training output is only as good as training needs data input. If the training needs have not been properly identified, then both the training course and the training are in jeopardy.

- The internal criteria must be in synchronization with the criteria used by the customer or organization. If the customer is expecting increased awareness and improved performance (reduction in security violations, increase in error free products), and the training function is evaluating the quality of the training output by different criteria, then the training system may be producing an unacceptable output as far as the customer is concerned.

Beyond Traditional Security Training

Under traditional or TQsT philosophy, the trainer and assistants must commonly perform the following functions:

The TQsT Function in an Organization

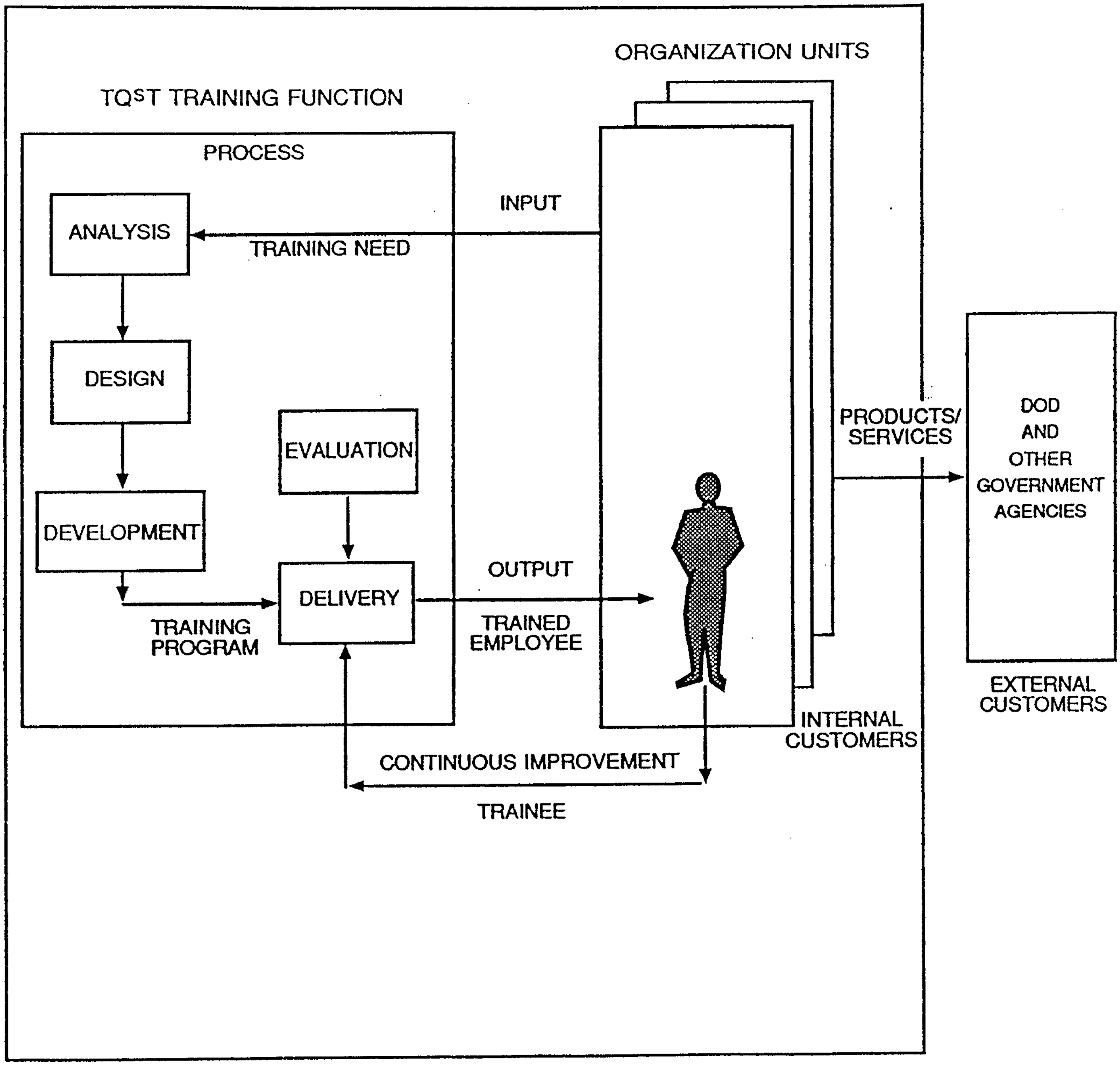


Figure 1

- Determine training needs;
- Develop overall plans, objectives, and assignment of responsibilities;
- Collect and prepare training materials, outlines, curricula, pamphlets, handouts, and audio visual aids;
- Teach certain courses (often orientation, indoctrination, and on-going security awareness courses) and select qualified instructors for others;
- Train certain operating personnel who are designated as instructors to develop teaching skills;
- Develop training programs in consultation with senior organization officials;
- Administer and coordinate all training programs; and
- Evaluate the effectiveness of the training effort.

How To Create and Maintain TQsT Results

We accomplish results and get effective training by following 10 cyclical steps of TQsT:

- Obtain and maintain management support and credibility.
- Analyze and clearly identify the actual needs of both the organization and its personnel.
- Develop a training action plan and present to management.
- Find and/or design and develop training material.
- Design a comprehensive measurement and follow-up plan.
- Select and train trainers.
- Validate the program with a pilot group.
- Collect data, analyze these, and adjust program.
- Implement the training program.
- Monitor and enhance the program over the long term.

Throughout this 10-step cycle, you must communicate with management to keep key officials informed of the progress and direction of the program. This communication is vital to maintaining your credibility as a valuable security management resource for consultation and effective solutions.

The **Figure 2** flowchart shows the sequential steps for TQsT. Notice the various times for communicating with management to retain the validity and credibility of your security training program.

Also, note the options for no training program. The first question to ask yourself "Is TQsT for me?" Only a lack of knowledge or skill requires education or training; any other reason requires management action of another sort.

The most critical phase of the whole process, however, is assessing needs and communicating them to management. The problem is often a conflict in how the needs are perceived. As a security trainer, you must understand your organization's goals and objectives, its abiding philosophy, and its vision, in order to identify the most important needs. At the same time, you must also be able to satisfy management with your solutions.

Where Does TQsT Fit?

TQsT is a complex activity which cannot be adequately understood from an external point of view. Much of TQsT may appear routine, requiring small plans of action, such as encouraging a student to demonstrate

TQsT Program Development Process

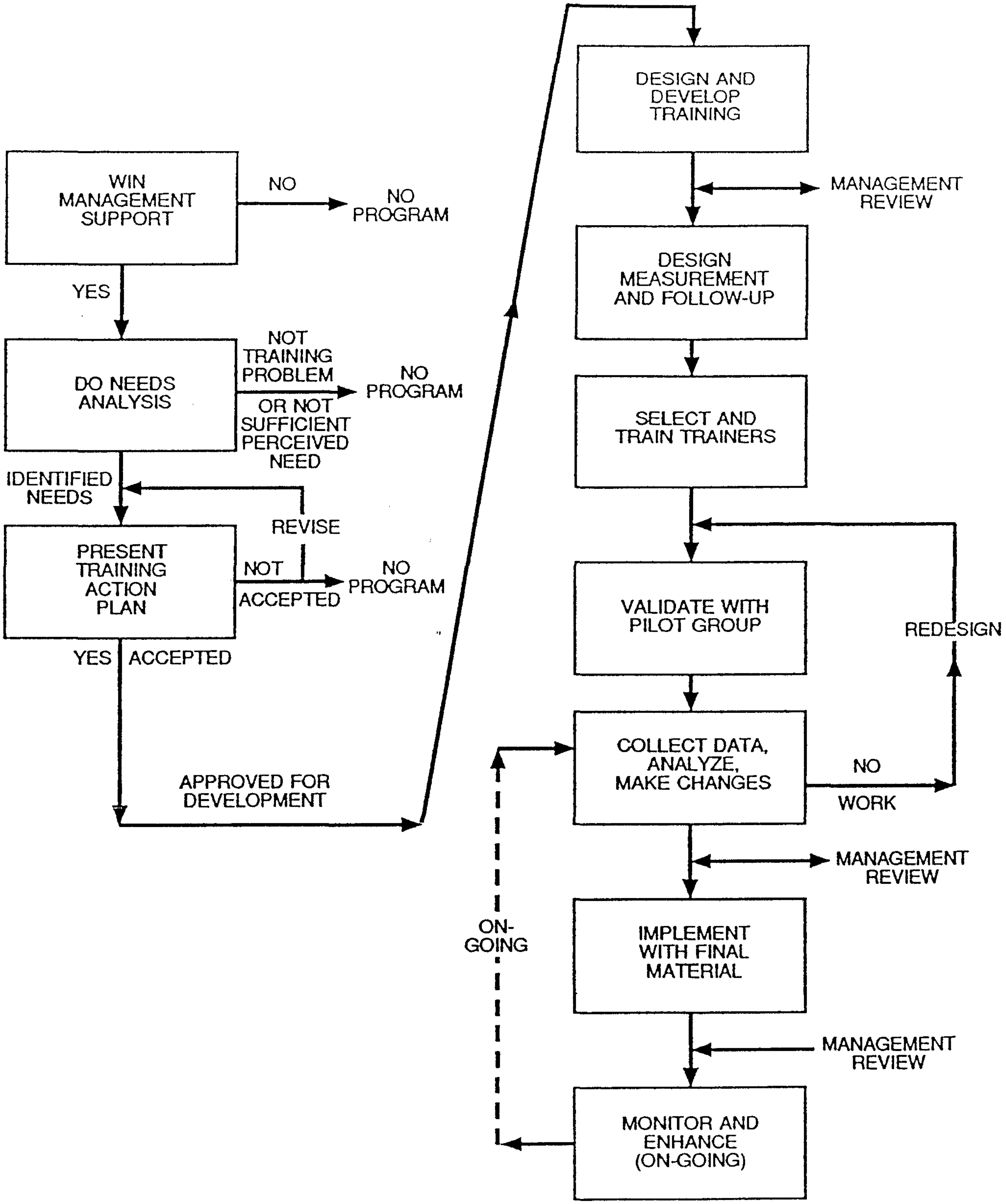

WIN MANAGEMENT SUPPORT
NO
NO PROGRAM
YES
DO NEEDS ANALYSIS
NOT TRAINING PROBLEM
OR NOT SUFFICIENT PERCEIVED NEED
NO PROGRAM
IDENTIFIED NEEDS
REVISE
PRESENT TRAINING ACTION PLAN
NOT
ACCEPTED
NO PROGRAM
YES
ACCEPTED
APPROVED FOR DEVELOPMENT
DESIGN AND DEVELOP TRAINING
MANAGEMENT REVIEW
DESIGN MEASUREMENT AND FOLLOW-UP
SELECT AND TRAIN TRAINERS
VALIDATE WITH PILOT GROUP
REDESIGN
COLLECT DATA, ANALYZE, MAKE CHANGES
NO
WORK
MANAGEMENT REVIEW
IMPLEMENT WITH FINAL MATERIAL
MANAGEMENT REVIEW
MONITOR AND ENHANCE (ON-GOING)
ON-GOING

Figure 2

competence by illustrating a classification marking concept graphically in front of his or her peers. Understanding the heart of security training cannot be limited to descriptions of trainers in action; what really matters are the intentions of training acts.

For example, what are the trainer's purposes in developing a cascading security training program during TQsT? The answer is obvious. A program such as this delivers training to everyone within the organization, in a cost effective manner. An added bonus is that the administrator of the program plays a significant role in the overall security posture of the organization.

The design, resourcing, and implementation of TQsT throughout the organization is easy. The stages in this TQsT model presuppose that the initial security training and education has already been administered. TQsT establishes itself in the realm of continuous security awareness by providing the employee with quality training throughout his or her employment with the organization. In **Figure 3**, preliminary planning and analysis is considered the most important part of the TQsT Program Model.

There are ten stages in the TQsT Program Model:

Stage 1 Security Program Analysis

Stage 1 is the study of the traditional security program as a theoretical framework for understanding total quality security training in the organization. The participants are pointed toward a full comprehension of TQsT as a basis of organizational excellence.

The objective of the analysis is to develop improved ways of resolving the security training problem empowering the employees of the organization, and by developing a security training blueprint that requires total employee involvement.

Stage 2 Executive Briefings

It is most important that the executive and senior decision makers of the organization are aware of the full importance and implications of security. This briefing should cover all those aspects of responsibility at this level, such as ultimate responsibility for security in the organization and original classification authority responsibility, to include annual training for certification. This briefing should also cover all those other aspects relative at this level and sketch out the method of disseminating TQsT and education.

Stage 3 Senior Management Education

An overview of the organization's security program theory and practice is presented to senior management, so that they are fully aware of the program and its contents. It is important at this stage to identify security policy and strategy, and to define all the central terminology.

Stage 4 Management Briefing

The main aspects of the organization's security program are covered in depth, based on the total security system. It is important that managers are fully aware, committed, and involved in all facets of the security program as it relates to their operational environment. It is also important at this stage to identify and define security responsibilities for supervisors, such as on-the-job training for their personnel.

Stage 5 Representative Selection

The organization structure of the activity should be considered and each major element (directorate, department) within the organization should have a security representative; this must be a person with the ability to inspire, lead, and facilitate a TQsT and education group. The security representative must have some ability, although skills, knowledge, and methods will be provided.

All senior personnel of the organization will

TQsT 10-Stage Program Model

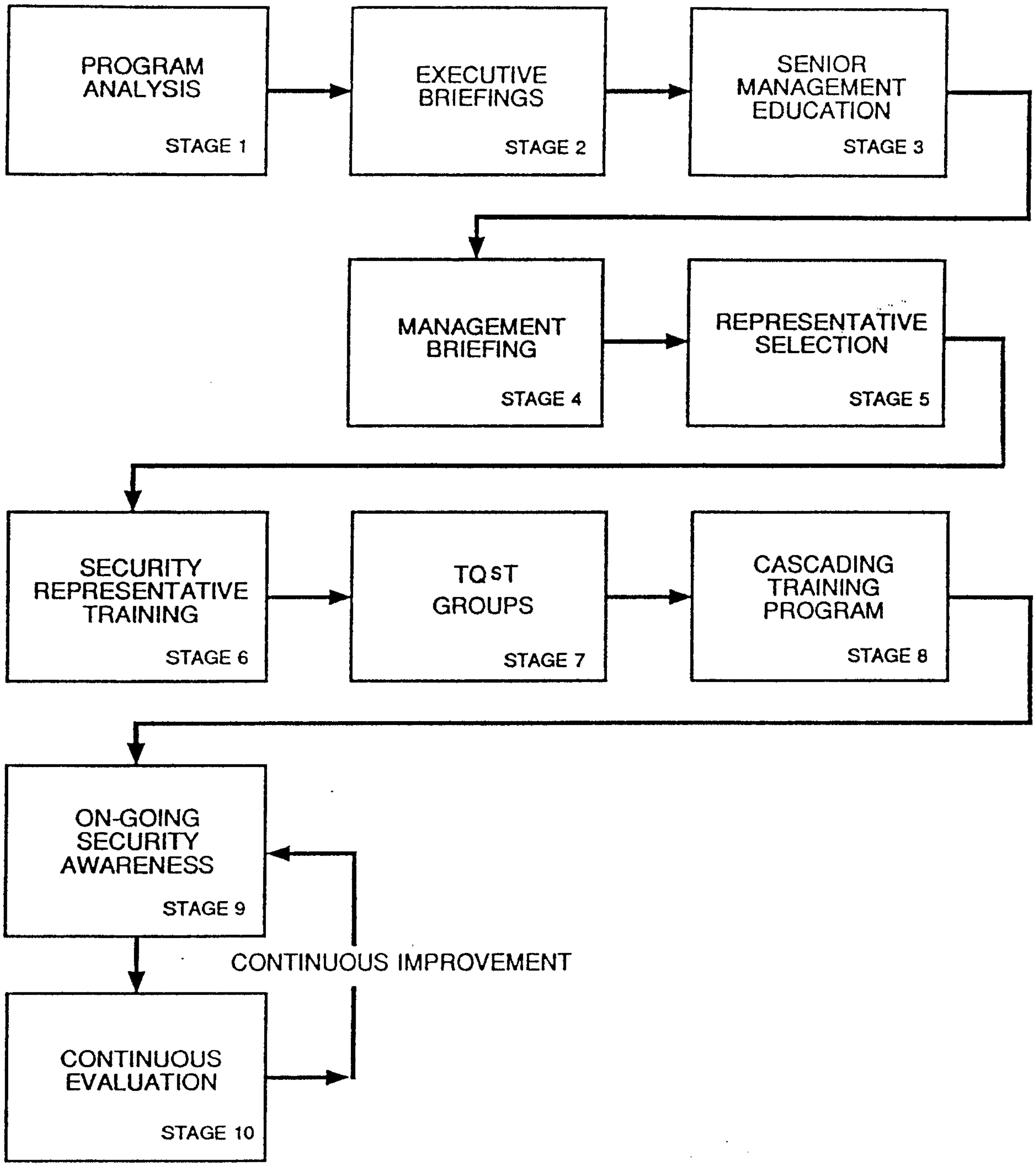


Figure 3

be trained by the security trainer or his or her assistants.

Stage 6 Security Representative Training

Security representatives are given Part 1 of the security representative training program. This imparts the necessary interpersonal skills and communication methods, together with a complete overview of the organization's security program.

Later, they will be taken through the TQsT program in a series of sessions, interlocked with the TQsT group sessions that they themselves will facilitate. These sessions will enable them to pass on the training to their own groups as outlined in Stage 7.

Stage 7 TQsT Groups

Regular meetings of the TQsT program groups are arranged. The pattern of these will reflect the elements of the organization. The security representative conducts training. It is vital that security representatives are provided with all the necessary materials and resources. They pass on the training from previous security representative sessions. (The organization's TQsT trainer and his or her staff provides such training.)

Stage 8 Training Program

The TQsT trainer arranges the training of security representatives, who provide the training to their groups. A TQsT trainer is also responsible for ensuring that the management training occurs simultaneously.

It is vital that all the necessary resources and facilities are provided and that all groups cover the same topics and with the same understanding, definitions, and priorities.

Stage 9 On-going Security Awareness

Regular meetings of the security representatives' groups are arranged. At these meetings, particular points, methods, and/or techniques are introduced for representatives to report back to their groups.

There will also be a need to update all new employees to the organization, at whatever level, to ensure that the organization does not become diluted with past bad habits and practices from elsewhere.

Stage 10 Continuous Evaluation

TQsT program evaluation encompasses five basic elements:

1. Identifying the decision makers who seek information and/or validation of the effectiveness of a particular training program (these people influence the budget and support the program, and it is essential that their expectations be determined in advance);

2. Clarifying the goals and objectives of the program, along with a specifically defined statement of their content;

3. Translating these objectives into criteria or standards for post--completion evaluation;

4. Creating a method for obtaining measurements; and

5. Interpreting the evaluation information provided by the measurements.

Making it Work

Few could see that we face increasing problems in the future with an inadequate understanding of change and its concepts. In addition, there are three implications that flow from this view of the TQsT function:

o If the security trainer does not analyze needs in terms of skills, cognition, and attitudes, then the methods used probably will miss the mark. "If you are not clear as to the target(s) you want to hit, you are likely to select the wrong arrows."

- Do not try to evaluate a given effort except in terms of specific target (or target mix) it is intended to impact (i.e., behavior, cognition, or attitude).

- When developing a TQsT program for upper management, be certain they know what they want to accomplish and can determine when these objectives have been fulfilled.

The resolution of these issues will depend less on rhetoric and more on action, but action is not likely unless people believe they can make a difference.

When looked at this way, enhancing security education and training helps build the personal and collective efficiency that helps us out of the entrapments of inequality that plague us in this very special venue. Needless to say, the hint of security education and training realignment along these lines may account for its absence in most of the rhetoric of the TQsT movement. Nevertheless, it is a powerful argument for Government and industry, which have a responsibility to extend education and training throughout the security community.

Closing the Loop

It is easy to be committed, but difficult to get results. The list of maxims presented at the beginning of this article is but a collection of suggestions. It is intended to focus concentration on the important issues facing security today. The organization of a total quality security training program is skilled work, and most organizations will need assistance if they are to reap the potential benefits and move into the 1990s.

Adam L. Gardner is the Security Training Specialist for the Naval Intelligence Command (now, Office of Naval Intelligence).

References

Articles

Chasteen, Charles A., William R. Whaley, and G.T. Gerkin. "Quality Resources: Cummings Grows Their Own," Technical & Skills Training. (October 1990), pp. 16-19.

Dodson, Robert L. "Speeding the Way to Total Quality," Training and Development Journal. Vol. 45, No. 6 (june 1991), pp. 35-42

Fisher, Kevin and Jo Ann Spillane. "Quality and Competiveness," Training and development Journal. Vol. 45, No. 9 (September 1991), pp. 19-24.

McDermott, Lynda C. and Michael Emerson. "Quality and Service for Internal Customers," Training and Development Journal. Vol. 45, No. 1 (January 1991), pp. 61-64

Reynolds, Angus. "The Basics: Total Quality Training," Technical & Skills Training. (November/December 1991), p. 11.

Rothenberg, Richard G. and Tom R. Drye. "Train 700 People in Quality? No Problem, " Training & Development Journal. Vol. 45, No. 12 (December 1991).

Simpson, Judith. "Visioning: More Than Meets the Eye," Training and Development Journal. Vol 44, No. 9 (September 1990), pp. 70-72.

Westbrook, Claud E. Jr. "Process Analysis, Employee Training Are First Stepes for Quality Program," Pulp & Paper. (March 1991), pp. 120-122.

Zagrow, Herbert W. "The Training Challenge," Quality. (August 1990), pp. 22-26

INFO-LINES

Beich, Elaine and Mike Danahy. "Diagnostic Tools for Total Quality," INFO-LINE, No. 9109 (September 1991).

Cocheu, Ted. "Training for Quality," INFO-LINE, No. 8805 (May 1988).

Younger, Sandra Millers. "How To Develop a Vision," INFO-LINE, No. 107 (July 1991).

TITLES AND AUTHORS OF PREVIOUS *VIEWPOINTS* ARTICLES

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

PART II - NCMS Viewpoints

Proposals for Improving Systematic Declassification Review
by Albert L. Thomas

Forcing Spies to Leave Messages
by Wes Lemmon

Security Awareness and Education: A Diversified Approach
by Diane A. Thomas and James J. Watson

Security Starts at the Top
by Neal W. Tuggle

Upgrading Security Classification and Extending Downgrading and Declassification Dates: Impact on Industry
by John S. Bowers

Incorporating the Control of Unclassified-Sensitive Information into the Defense Industrial Security Program
by James J. Bagley and Charles H. Kocher

Let's Take a Good Look at Classified Visits
by Jeanne Bastoni

Security Education in the Defense Industrial Security Program: An Underused Tool
by G. Ernest Govea

TITLES AND AUTHORS OF PREVIOUS *VIEWPOINTS* ARTICLES

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

Holistic Security Management: U.S. Government and Industry Planning for the Year 2000
by Paul M. Joyal

The Department of Energy's Personnel Security Assurance Program: Its Purpose, Design and Effect in the Workplace
by Lynn Gebrowsky

The Denial of FOIA Requests for Unclassified Security Vulnerability Assessments and Classification Guides
by Ronald W. Marshall

Determining the Effectiveness of Security Awareness Programs
by Peg Fiehtner

NISP: Assessing Today's Security Reality and Recreating a Vision for the Future
by Maynard C. Anderson

Limited Dissemination Controls are Not Special Access Programs
by Raymond P. Schmidt

The Threat to Western Technology
by James W. Dearlove

TITLES AND AUTHORS OF PREVIOUS *VIEWPOINS* ARTICLES

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

NCMS Guidelines for Submitting Articles for Publication

- Submit four copies of each article.

- If possible, include a 5-1/4 inch floppy disk using WordPerfect software.

- Type with double-space and generous margins.

- White 8-1/2" by 11" paper must be used.

- Cover page should provide a title and any desired subtitles, but no personal identifying information about the author(s) to ensure objective consideration by the NCMS *Viewpoints* editorial review board.

- Forwarding letter(s) should be signed by the author(s) to indicate that all the required information is included and all material has been reviewed for accuracy and completeness.

- Signed forwarding letter should also bear this statement:

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

- Name(s), address(es), telephone number(s), and any other personal identifying information [*e.g.*, biography(-ies)] should be in the forwarding letter or on a separate sheet of paper, but not on the manuscript.

- Acceptable subject matter encompasses the broadest range of professional information appropriate to NCMS members.

- Commonly-accepted professional standards of propriety, civilized discourse, and discretion should be observed.

- No specific length is established, but authors should include both illustrations and aids to editorial reduction for particularly extended dissertations.

- Please note that NCMS will copyright the published article, but author(s) will be allowed to reprint without restriction.