VIEWPOINTS

C

M

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. 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.

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

Last summer NCMS members received a bonus in the annual *Journal:* eight excellent articles by ten authors who addressed security management; industrial security; awareness, training, and education; systematic declassification review; classified visits; and controlling unclassified sensitive information. If you overlooked them, those thoughtful pieces are located in the last ten pages of your *Journal.* I believe the professional dialogue in them is worth investing at least an hour of your time.

Now, thanks to our many talented members, you are about to enjoy another collection of provocative items. Each was read and approved by the *Viewpoints* editorial review board. Individually and collectively, these articles challenge us to think about our roles as security specialists. They examine current issues of security importance that will help us prepare for the millennium.

The initial piece stimulates us to look ahead to the year 2000 and envision the security needs of government and industry. Paul Joyal submitted this paper in 1990, before much of the political restructuring of Europe. His experience on the staff of a Congressional committee and as a private consultant give him a unique window on the future. He is already working on another item for a future edition of *Viewpoints*!

James Dearlove has delivered his briefing on the loss of our technology to key officials and general audiences both here in the United States and abroad. Although he worked hard to bring it up to date regarding international events and the names of officials, no one in the past two years has been able to predict accurately what would happen next in Eurasia. On the other hand, most of us will be surprised at his description of the increasing outflow of vital technology. The article printed here reproduces many of his graphics, but cannot capture his vitality. Nevertheless, the picture he paints gives further credibility to Paul Joyal's concern about the future.

NCMS members will immediately recognize Maynard Anderson as the senior Department of Defense official most closely associated with security policy over the past decade. Some of us have heard him talk at annual seminars and other forums. His recounting of a brief history leading up to the National Industrial Security Program suggests that serious high-level attention is being given to the problems we face. We may be somewhat better off than that frog in the hot soup, *if* we remember to cooperate!

Ron Marshall introduces a little-known but potentially powerful fact about Freedom of Information Act exemption two. The legal citations will help those who wish to verify for themselves the findings of each case. The bottom line, however, is that security specialists may be able to use the "high two" exemption to deny access to unclassified documents that are closely related to the national security.

Lynn Gebrowsky describes personnel security measures that will be familiar to most of us. Despite its brevity, it carries a message that these procedures require an attentive security manager.

Peg Fiehtner addresses another critical issue that demands time and attention of the security manager. Security awareness requirements may seem to have an obvious solution, but most of us will find at least one new suggestion in this piece.

The final article attempts to distinguish between special access programs and a relatively new security measure known as limited dissemination controls. It has been improved by the generous constructive criticism of key officials in the Department of Defense and Department of the Navy.

Some readers may feel just a twinge of frustration at not being able to discuss or debate issues with any of these authors. You can overcome this feeling by writing your own article. Expand upon, challenge, or develop an alternative argument. *Viewpoints* was conceived to inform and to stimulate creative expression of divergent points of view. This is the first stand-alone edition of this periodical since I was asked to assume editorship ten months ago, in February 1991. NCMS is large enough and its members sufficiently mature to accommodate members who have different professional convictions. Please do not hesitate to submit your articles, letters, and other literary contributions.

Raymond P. Schmidt
December 1991

P.S. As this issue of *Viewpoints* headed toward the printer, President George Bush signed the following brief memorandum to the Secretaries of Defense and Energy and the Director of Central Intelligence:

"Thank you for your report on the National Industrial Security Program.

"The government-industry taskforce you established has made considerable progress toward development of a single, coherent, and integrated program. This remarkably collaborative effort between government and industry will lead to significant improvements in the security of our Nation.

"I am especially pleased with the projected time frame in which you intend to fully implement this vital program, which will provide cost-effective and secure development and delivery of systems essential to our national security."

HOLISTIC SECURITY MANAGEMENT:

U.S. GOVERNMENT AND INDUSTRY PLANNING FOR THE YEAR 2000

Paul M. Joyal

Introduction

We must redefine and restructure the several *security disciplines* in the 1990s so they become fully *integrated*, helping security achieve *professional standing* in the eyes of the U.S. Government and industry. By the year 2000, the artificial distinctions among information, personnel, automated and physical security disciplines must disappear, creating a *unified management instrument* that allows managers to provide security protection in depth for things of value. This *unity* will better position us to meet the threat to U.S. national security which comes not only from foreign agents, but also from trusted employees who volunteer to spy on our country.

We can no longer tolerate the traditional parochialism, restricted experience, and narrow educational paths of security specialists that continue to dog our every step toward mutual support and improvement. Top leaders in government and industry must develop career paths that allow rapid and full development of the best young persons we can attract to meet our coming challenges. This *new security professional* must possess a blend of skills found in the computer analyst, personnel specialist, manager, educator, social worker, counterintelligence officer, and detective, to name a few.

Such dramatic and revolutionary changes are essential because contemporary organizations have the ability to produce information that far outstrips their ability to control it. Ironically, the very same factors which created the information explosion are causing the current severe crisis in information security. Automation, electronic transfer, rapid reproduction, microminiaturization, and satellite relays allow individuals and organizations to communicate and handle far greater volumes of information than security specialists normally cope with--or even comprehend. Consequently, one challenge in our future is to deal effectively with the expanding *environment of databases* which yields significant insights into classified work centers and their functioning. We can come to grips with the larger challenge best by first tackling the key dual problems: physical control of classified documents, and consistent safeguards for classified information--as well as unclassified but sensitive information.

Background for Sizing Our Current Problems

The public revelations of successful espionage conducted against the United States in the post-Vietnam era reached a climax in the 1985 "year of the spy." It became ever more evident that security had been seriously breached in both government and industry. Over the next several years it seemed that no organization was immune.

For example, the Navy broke the John Walker ring and caught Jonathan Pollard red-handed; CIA contended with Larry We-Tai Chin and Edward Howard; NSA brought Ronald Pelton to trial; the Marines court-martialed Clayton Lonetree; the State Department dealt with Felix Bloch; the Army with Joseph Helmich, James Hall, and Clyde Conrad; and the Air Force with Edward Buchanon and Allen Davies.

Adding more fuel to our concerns, the full list actually was much longer and has continued to grow. Understandably, these insider-spy cases focused our attention inward, perhaps even to the point of neglecting the continuing threat of external espionage. Observers feared that an ever-expanding group of citizen-traitors, motivated by greed and revenge, would now pose a greater threat than foreign agents--or even turncoats who are driven by political ideology or party affiliation.

Subsequent studies and reports have given little comfort in reducing the scope of our concerns. The Stilwell Commission Report, prepared for the Secretary of Defense in November 1985, made sixty-three recommendations to reduce security vulnerabilities and provide remedies for the problems it identified. The Senate Intelligence Committee issued "Meeting the Hostile Intelligence Challenge" to express congressional concern, and to provide solutions for the vexing spate of apparently unstoppable leaks. Hundreds of similar recommendations emanated from various sources, each attempting to address needed improvements in the information and personnel security programs of government and industry.

The Nature and Scope of Threats to Our National Security

Espionage remains a serious threat to the existence of the United States and increasingly threatens to undermine the standard of living of every U.S. citizen. Judge William Webster, the Director of Central Intelligence, pointed out at the National Press Club on 29 November 1989:

"Around the world our stations are reporting more aggressive action, a more robust intelligence collection effort to recruit our embassy and intelligence personnel than we have seen in a long time."

He continued by noting that the recent Soviet spy effort is less confrontational, but the methods used should not lead one to conclude that the level of their activity has decreased. On the important issue of *technology transfer*, Judge Webster observed:

"And as less money is dedicated to that particular effort inside the Soviet Union, more and more efforts need to be applied to obtain that kind of technology through clandestine means."

Similarly, economic competitiveness is a strategic concern for our Government. We are all aware of the long tradition of *corporate industrial espionage.* It may become even more harmful to us in the years ahead. President George Bush in his March 1990 *National Security Strategy of the United States,* reiterated how national security and economic strength are indivisible, and how our economic and military strength rests on our technological superiority. *Business Week* reported on 28 September 1981 that at least three spy schools in Japan and Switzerland were turning out graduates in industrial espionage. American companies were considered "soft targets." *Fortune* magazine reported on 26 July 1982 how Hitachi and Mitsubishi conspired to acquire IBM technology illegally, and were apprehended in an FBI sting operation which the magazine termed 'JAPSCAM.'

Senator David L. Boren, chairman of the Select Committee on Intelligence, explained that *economics* will play a more prominent role in worldwide intelligence collection during the 1990s. Addressing the National Press Club on 3 April 1990, he observed "As the arms race is winding down, the spy race is heating up [and accounting for]...an increasing share of the espionage directed against private American companies, [and] aimed at stealing commercial secrets to gain a national economic advantage."

In the early 1980s the Reagan administration learned through particularly sensitive sources that the Soviet Union was engaged in a massive and sophisticated effort to acquire the West's most *critical technology.* The facts were detailed both as to the USSR's organizational structure and procedures, and to the targets of the effort. In May 1982, the administration provided indications of this massive Soviet global industrial theft program to the Senate.

Subsequently, in 1985, many of the details about these successful Soviet espionage efforts were published in *Soviet Acquisition of Military Significant Western Technology: An Update.* It is one of the most extensive reports ever issued. Several shocking statistics will serve to illustrate: Between 1976 and 1980 over 3,500 technological informational requirements were filled; another 30,000 pieces of military and dual use hardware and some 400,000 technical documents were obtained by these nefarious efforts. The 1985 report concluded:

"Even if there are managerial reforms, no real lessening of the Soviet dependence on Western innovation is anticipated as long as the U.S.S.R perceives the need for *military technological parity* with the West, or the need for superiority. The impact of this dependence could be even more important in the 1990s than it is today. The U.S.S.R has been compelled to follow Western direction in technological change[, but] ... the next decade (1990s) is less certain for the Soviets."

We have no indication that this *Soviet dependence on Western technology and innovation* has changed. Some may argue that even the limited recent effectiveness of the West's security efforts, while not stopping the exodus of sensitive Western technology, has made the cost prohibitive for the Soviets to pursue into the indefinite future. This fundamental USSR dependence must be addressed internally. These may be factors in the Soviet efforts to create a new image and encourage democratic trends in the eastern European Bloc of Soviet satellite states.

The emerging changed relationship between the Soviets and the Bloc will force the *Soviets to compensate* for the loss of the once manageable and effective *surrogate intelligence service* of their *client states.* President Vaclav Havel of Czechoslovakia has reported that he recently signed an historic agreement with the Soviets prohibiting any future joint intelligence operation against the West. According to Dr. Larry Bittman, former Czech intelligence officer, this is the most important indication yet as to the real changes occurring in what was the Warsaw Pact Bloc.

The "one Germany" will pose an even more difficult challenge. In an unusual, rare interview with *The Washington Post* on 19 November 1989, the legendary former head of the East German foreign intelligence service, Markus Wolf, predicted his own profession of foreign espionage will continue to thrive: "If the military confrontation diminishes, then we can *change the tasks of spies abroad.*" The overriding task of intelligence, he continued, "is to prevent unpleasant surprises." Perhaps with a note of irony, he asserted that during a period of relaxed international relations, espionage "improves the chances for peace" because neither side "believes it can develop a weapon or secret strategy without the other knowing about it."

When Judge Webster was asked to comment on the status of the Bloc intelligence services, he wisely noted that "it is much too early to tell how quickly those intelligence services will erode."

As world tensions relax and the once formidable barriers to human movement disappear, numbers of *visitors and emigres* will increase. This will certainly challenge our ability to cope. Soviet emigres to the United States were only 6,800 in 1987. By 1989 the number jumped to 43,500. Again, Soviet visitors to the United States were only 6,849 in 1987. By 1989 the number had jumped to 47,365. These are merely one indication of the human resource challenges, and the scope of potential threats to our national security.

Another aspect of the foreign intelligence threat derives from new capabilities in *electronic technology.* Lieutenant General Harry E. Soyster, Director of the Defense Intelligence Agency, while addressing the northern Virginia chapter of the Armed Forces Communications Electronics Association on 27 October 1989, stated that the Soviets are making a concerted effort to access our most sophisticated state of the art computers. These targets include "scientific and technical developments, energy sources, and industrial research and design manufacturing processes [...to include] microelectronics fabrication equipment and computers."

Defense News reported a speech by Michelle Van Cleave of the White House Office of Science and Technology that reveals yet another dimension of the threat: "Nor are the East Bloc the only powers seeking American business and financial data." Other nations frequently share these data with their private businesses, both formally and informally. Recently, Australia arrested three persons for tampering with computers in the United States and Australia.

Government and private U.S. companies must be cognizant of the dangers in obtaining information in even in domestic competition. The front page of *The Washington Post* business section on 21 February 1990 proclaimed "FBI Probing Claims US Sprint Obtained Confidential Material." The article went on to outline the investigation of the alleged plot by US Sprint to obtain information "through a tap of a government computer that helped it win a federal phone contract potentially worth billions of dollars." In January 1990 the Associated Press reported that three Silicon Valley computer workers were indicted for breaking into a Government computer and obtaining classified military data.

It should be obvious by now that the espionage threat is real and steadily becoming more sophisticated. The case of the Hanover Hackers illustrates how a group of skilled agents can be tasked by a foreign intelligence service to break into remote computers with the intention of committing espionage. In this case, only the persistence of a private citizen led to the identification of the face of espionage. As a footnote to this case, a hacker involved in the West German ring, Karl Koch, was found immolated in a ditch outside Hanover. Incredibly, Koch has been described as the apparent victim of a suicide!

The *hostile espionage threat,* whether by foreign governments or our own citizens, against U.S. military, industrial, and economic information is clearly *increasing.* Decreasing tensions between the superpowers encourages us to think that we may be on the way to a more peaceful world, but competition and opportunities for espionage are apparently increasing. President Mikhail Gorbachev's aggressive worldwide public relations campaign for a time gave us a perception of a more peaceful and friendly Soviet Union. Not surprisingly, this brought more foreign visitors and emigres to the United States, and greater opportunities for Soviet espionage operations and recruitment. This relaxed atmosphere is conducive to volunteer internal aid to the Soviets, and to employee rationalizations for treason motivated by greed. Once again, the threat of the insider within our trusted employee systems must be emphasized.

With these rapid and fast-developing changes, we must be open to the possibility that those who are our adversaries today may not be in the future. And conversely, those who are allies today may be our adversaries, whether military or economic, in the future. This calls to mind the statement by the late General Charles DeGaulle that nations do not have allies; they have only interests. In appreciation of these factors, a new security infrastructure is required.

Our conception of the threat must keep pace with rapid changes to the international landscape. For example, will the classical hostile intelligence designations still apply? Looking at the economic deprivation of Eastern Europe, could the changes there turn their foreign intelligence services into industrial espionage establishments not subject to Soviet direction? Indeed, will these services direct their attention to new objectives of supporting domestic economic development? Or will we see the emergence of a Bloc contract business, offering an industrial espionage service to clients? Looking at the focus of their efforts, will these services target more economic and technological intelligence over the next decade?

The answers to these questions will have a direct and immediate impact on how the security profession evolves during this period of transition, especially in industry. We can hope that they will contribute to a new conception of corporate security for U.S. companies. Traditionally, the focus of security programs has been on protecting Government secrets. What we need for the future is an expanded vision which views the entire company comprehensively. Security can no longer be an appendage to administration or operations, but must be the catalyst that integrates the protection of proprietary, financial, technical, and strategic information with the more traditional information, personnel, and physical security disciplines of the past.

It is with this vision that I introduced the phrase holistic security a few years ago. The year of the spy and my work at the Senate Intelligence Committee convinced me that a more comprehensive approach was required to meet the espionage challenge. The selection of the term holistic attracted me for its connotation with health. Security should endeavor to protect and advance the well being of the institutions it serves. With this I turn to some of the lessons from what became the decade of the spy.

Security Lessons Learned from the Year of the Spy

Our leaders clearly recognized that U.S. security programs must be improved to meet the espionage challenge revealed by the obvious serious lapses in personnel security. It is the burden of this essay to argue that we cannot address personnel security issues in isolation; rather, we need to combine their resolution with effective protective measures from the other security disciplines. Viewing problems raised over the past decade from our standpoint as officials in Government and industry, we are able to address personnel security realistically only when a cleared individual enters the national security establishment. Once begun, the personnel security program should continue throughout the active service of each individual. Equally important, however, we must accept our responsibility to address personnel security even after the individual separates from classified work or active government service.

Significantly, the Personnel Security Research Center was established within the Department of Defense with Navy funding specifically to find ways to identify potential traitors before they are allowed to enter into classified duties. Another proposal put forward was to place greater reliance upon the polygraph as a formidable and important instrument of deterrence. The polygraph is widely acknowledged as an important instrument for conducting an effective security program, although it is not universally accepted as sufficient, in and of itself.

Experience also suggests that we should refine two other useful tools for achieving better security. They involve limiting access to classified spaces and imposing positive controls for access to documents. The document control system must be able to collect data to match specific item use profiles with records of actual access by individuals to key documents and related information. These in turn must be correlated with the need-to-know requirements of individuals. Both integration of document controls with individual access records and the automation of these data are needed.

The Pollard case illustrates what can occur when adequate need-to-know and document use controls are not in place. Pollard exercised his ability to raid data bases at will, violating the need-to-know principle. He was able to remove highly sensitive material from various facilities for offsite reproduction by avoiding the enforcement of authorization and accountability procedures. Finally, Pollard's facility security officer woefully failed to enforce strict personal storage accountability rules, and did not maintain adequate records showing Pollard's access to specific documents.

Given this background of the 1980s, I see one key question emerging from that experience: How can we reshape the security rules and regulations developed during the post-World War II era to give security managers adequate counterintelligence detection capabilities in the 1990s?

What Can be Done?

As mentioned above, information and personnel security are not separate and distinct, but are closely related and must be used in conjunction with physical security. I will outline seven strategic issues and suggest steps that can be taken to make sure that the security disciplines are integrated.

First, the issue of what is classified:

The Government should continue to improve its identification of what is classified in the interest of national security. The definitions must be sharp and clear so our limited resources can be committed to protect classified information better with improved document control and physical security systems. Conclusions drawn from previous and additional damage assessments could aid in this process.

Second, the issue of developing workable security systems:

We need a Government clearinghouse within a designated federal agency that provides cost and performance information relating to physical security equipment and new, emergent technologies that will improve the integrated security programs. The clearinghouse would test, evaluate, and demonstrate the new systems. It could make grants to offices and organizations that are seeking to impose creative solutions to difficult or multi-layered security challenges. Agencies may volunteer to act as test beds for new equipment and technologies using the holistic security approach that I will describe subsequently.

Third, the issue of calculating and programming security costs:

Executives and managers need to consider that security is a direct and necessary cost in future government projects and contracts, especially those that make major demands on protective measures. Information, personnel, and physical security should be factored into the upfront cost of projects and contracts, as well as in all offices handling special access material; it too often is an additional item tacked onto project or contract totals, and faces the first cuts when times get tough. The new security professionals must develop the necessary administrative techniques and skills so they can calculate the physical and personnel security costs per job, mission, and project or contract.

Fourth, the issue of professional stature for security people:

At the heart of the security program, the security manager or security officer ought to be well educated and experienced in the security disciplines and in the work of the organization.

Security specialists deserve the same career opportunities as their colleagues in the organizations they serve. Perceptive senior executives and managers recognize that a well trained security tions they serve. Perceptive senior executives and managers recognize that a well trained security staff is not only a cost saver, but also the best insurance against espionage and a prophylactic against damage to the national security or free-world economy.

Fifth, the issue of a national industrial security program:

Today, we sorely lack a clear, comprehensive and unified set of rules, regulations, and standards for information, personnel, and physical security in the industrial sector of the national security establishment. Why do we keep multiple sets of books, one for each entity conducting an inspection or managing the contract? The woefully inadequate Executive Order 10865 could be reissued to create a strong, comprehensive, and uniform national industrial security program. Presidential leadership is essential if we are to eliminate the often confusing and frequently duplicative policies which govern the current programs.

Our industrial security policies need to be streamlined with one set of criteria and common adjudicative and due process procedures for clearances, simplified and clear physical security standards, common inspection guidelines, and training and certification of corporate security officers. The goal is dramatically increased cooperation between Government and industry in defining, executing, and enforcing policy. This creative holistic approach would save resources and directly benefit the national security.

Sixth, the issue of holistic security in special access programs:

Offices that administer special access programs should remain current on new security technologies that could be implemented. Annual feasibility and desirability studies can show whether creative approaches to document security and physical security will reduce costs.

Seventh, the issue of paying for better security:

While the previous issues are being resolved and once steps are under way to integrate the security disciplines under a holistic set of policy guidance, agencies that administer programs requiring a high degree of security must program sufficient resources for classified projects and contracts. The Government must shoulder its fair share of the security burden if it expects results, and industry must clearly lay out security costs at the time it bids on a contract.

Proposed Characteristics of a New Holistic Security Model

Our present security structure lacks unity. It cannot effectively control, track, and protect classified material because it does not have the characteristics of a system: a set of interrelated, interactive, or interdependent parts that work together to create a whole.

The Battelle Institute has formulated an integrated, or holistic, concept known as the *Information Control Unit,* or *ICU.* The ICU acronym is apt because the image of intensive care applies. Battelle created a model system which integrates the various components of physical security and document protection into an ICU, and links ICUs to form an unbroken chain. Beyond linking of units, the Battelle ICU envisions that its model will include an effective loss or compromise detection capability to forge crucial synergistic relationships between personnel security and physical security.

Whatever the model or paradigm is called, a holistic architecture for a new security structure should possess these five minimal features:

1. Document accountability, with internal controls on all classified material transactions, personnel access, and storage authorizations.

2. Internal control procedures, governing all access to classified material and tracking the transfers of classified material.

3. Multiple protection safeguards for reproduction, regulating the copying of classified information (an application of the "security in depth" principle).

4. Media storage devices and classified material identification techniques (*e.g.* bar coding, RF/ID tagging), to help prevent, detect, and pinpoint or isolate unauthorized removal.

5. Destruction and external removal of classified material, to enforce the same strict account-

Any new security structure must also streamline the U.S. industrial security program to establish one set of standards for personnel clearances, common adjudication and due process procedures, a common basis for physical security standards and inspections, coherent training guidelines, and uniform certification procedures for corporate security officers, to mention some of the most pressing issues.

Specific Building Blocks of a Holistic Security System

In order to achieve the firm accountability for individual documents and conduct smooth internal control procedures, I recommend several building blocks that are discussed under three general headings.

First, repository control measures should lay the need-to-know foundation within the work center or larger organization that is essential for controlling access to classified information. Some of the basic points to consider are these:

1. Documents enter the work unit through the security office and are entered into a central register for accounting.

2. Personnel are sub-divided into classified knowledge compartments based upon job or task requirements.

3. The resulting data base is compartmented according to the need-to-know principle.

4. Personnel can acquire classified documents on a daily basis through the security staff.

5. Documents could be stored in a central or several decentralized vaults or safes and checked out or accounted for on a daily basis either personally or electronically.

Second, individual document control would entail taking the following steps to facilitate document and access control:

1. Apply bar codes or a similar identification to all documents, tapes, and storage media when they are processed into the organization.

2. Portal monitors (antennas) could read the tagged bar codes or other RF/ID tags upon entry and egress for routine verification or notification of security.

3. Documents are made available to individuals on the basis of a need-to-know.

4. Using the data collected, individual document review can be conducted real time and over time.

5. Special inks, toners, or paper could be used containing an inert material that is detectable by an electroptical or ultra-violet sensor.

6. The treated paper, used in conjunction with reproduction authority and a sensor on the printer, could block or approve each reproduction job, or monitor duplication.

7. Sensors could correlate the bar coding on a document with the operator of a specific reproduction machine.

Third, physical access by specific individuals to classified documents could be controlled in several ways:

1. Digitized fingerprints for biometrics readers, combined with smart and proximity card technology, could provide a detailed history of movement through and/or within a special facility.

2. Access to a facility could be biometrically controlled. A combination proximity/smart card could track internal movement and customize individual access profiles. A proximity/smart card could also contain the digitized fingerprint of the bearer. This could interface with the biometric device installed on the reproduction equipment to track and authorize reproduction. This card might also contain a video image of the user and his or her clearance and access history.

3. Portal monitors could be installed at choke points to record both authorized and unauthorized removal of classified material. By linking material removal with the proximity/smart card,

verification of each transaction can be remotely accomplished.

4. Adding certain inert material into laser print toners may also permit the capture of images through briefcases and other opaque surfaces. Once subjected to a multiple-hued imaging x-ray machine, classification markings could be captured. Other research should be conducted into various remote tracking capabilities.

Conclusions

Our problems stem from inadequate management of the tremendous streams of data and information. We need to obtain greater accountability and tracking of classified documents and data bases. As Shoshanna Zuboff of the Harvard Business School describes in *The Age of the Smart Machine: The Future of Work and Power,* information technology not only produces information, it collects information. Our task is to seek creative ways to analyze the collected information for use in security.

We must find ways to put to work, for our advantage, the new technology and new systems that created the problems associated with the modern electronic office. Expert systems and artificial intelligence should be made to serve us by helping to identify anomalous and problematic activity. Event-initiated programs could provide the security manager immediate indications of the precursors to trouble--or espionage. Our goal is to spot potential problems and prevent commission of criminal activity.

Security managers must develop new skills pertinent to the age of the smart machine and the ubiquitous, if vulnerable, database. The manager in the year 2000 will need a strong theoretical understanding of the integrated security discipline, and of the automated information system environments. These data-rich environments require clear understanding of the internal links, relationships, and associations -- as well as what data are available, how they are accessed and analyzed, and how they might be related to other sectors of data and events. Our new manager will interact directly with data bases, analyze what is happening, and develop ideas and concerns for further inquiry. The higher level skills required include data-based inferential reasoning, procedural reasoning, and the limitations of pure deductive reasoning. Training must take into account the fact that security assessments will no longer be organized according to functions and occurrences. Our security manager ten years hence must comprehend the structure of the data base environment and the security implications of how data bases work.

Only a holistic approach to security will enable security managers to see and solve problems on a global scale. The new technology forces the security manager to take a broader view. This will enable the manager to identify patterns in the sea of data, and determine the relationship of specific patterns to the whole phenomena. Connectivity and flexibility will relate the computer to the manager through physical access control, document control, information security, and personnel security.

Security must redefine itself as a profession to accommodate the new broader perspective, and overcome its limiting self-image as an extension of law enforcement. Within this decade security professionals can become the "renaissance managers" of the corporate culture. This is not only a tall order, it is essential if we are to meet the growing espionage and hostile intelligence challenges by the year 2000. Security works best if it is holistically linked to the entire company. After all, a well balanced and integrated security posture is not simply the protection of certain "secrets" but relates to the well being of the entire organization, its personnel and material.

From a personal perspective, security specialists will often need to confront their "natural attitude" which uses past tools and ways of thinking to meet radically different challenges. It is natural to take for granted the objects and activities that surround us, because this enables us to live our daily lives. The "natural attitude" becomes a treacherous enemy, however, when it leads to inertia and prevents us from tackling unexpected situations in fresh terms. Critical to success in meeting this psychological challenge is to examine our operating significance when solving holistic problems.

Finally, as Shoshanna Zuboff has advised, our greatest need is for leaders who can move us in the direction that accommodates the technological advances in both our working environments and our personal orientation. They must be able to recognize the historical moment seen in the perspectives of time, place, and the alternative choices presented. Most importantly, they must be able to make organizational innovations that can exploit the unique capacities of the new technology, and thus mobilize organizational potential to meet the heightened rigors of worldwide competition. These leaders can make the crucial difference between being stranded in a new world with old solutions, and forging new paths of creative problem-solving. Without such leaders, we will fail to understand the new technology and must suffer through the avoidable vicissitudes of its consequences. Clearly, new visions of organization and work offer us dramatic benefits if we can grasp them. ■

Paul M. Joyal is Vice President for Security and Technology Programs, Washington Consulting Group, and formerly Director of Security, Senate Select Committee on Intelligence.

THE DEPARTMENT OF ENERGY'S PERSONNEL SECURITY ASSURANCE PROGRAM:

Its Purpose, Design and Effect in the Workplace

Lynn Gebrowsky

On a typical day Janie Halstock[1] arrives at work at 7:00 a.m. She parks her 1989 Dodge in the parking lot, along with 500 other cars, pick-ups and motorcycles, and goes to her work site. At this point, all similarity between Janie's morning routine and that of most other Americans ends. To get into her work area, Janie passes through some of the tightest security controls imposed on any industrial population: detectors, guards, fences, access control devices, and, some days, a search of any items she may be carrying. She changes into work garments covered by a suit of protective clothes. Around her neck is a respirator. Once at her work station she is observed by cameras, a watchful supervisor and a handful of fellow workers. To do her job she must reach into a "glove box," her hands sheathed in neoprene gloves. The glove box is a 50" X 30" X 37" box, its interior under negative pressure to prevent the contents escaping into the room. All of this security is necessary because Janie works at a Department of Energy site, processing materials used in the production of nuclear weapons.

Throughout the United States, there are many people doing similar sorts of jobs under similar conditions. Some process materials, some perform chemical processes, some do fabrication, some machine material. All of them are dealing with what is termed "special nuclear material" (SNM). Significant quantities of SNM are referred to as being Category I quantities. Without being technical, Category I quantities of SNM are those that could pose an extreme danger in the wrong hands. Another way of looking at such material is to describe it as highly valuable to certain individuals, organizations, and governments. These materials are both dangerous in and of themselves and are highly desired by persons or groups whose interests may not be those of the United States or of the company where the material is handled. Such hostile people or groups may also pose a risk to the health and safety of the company employees and the general populace. These two factors, the desirability and the hazardousness of SNM, create a potentially volatile mix.

It is in response to this threat that the physical security measures to which Janie and her co-workers are subject were developed. There is, however, another dimension to this issue of protection, and that dimension is people: Janie herself and her co-workers and supervisors. And there are people outside of Janie's work site who are also part of the overall process of creating and utilizing SNM. There are guards who protect the material and oversee its transportation. There are also high-level supervisors who are responsible for directing personnel and actions and who have the capability of manipulating the system.

One way of addressing the dimension of people is through the personnel security clearance process. This is a time-honored method and a very effective way of determining a person's past actions. The traditional personnel security clearance process used throughout the Department of Energy (DOE) and other federal agencies is based on a background investigation combining records checks and source interviews. From looking at past actions, a picture of the person can be drawn. Such a picture, however accurate, is essentially static: an image fixed in time. People are not fixed in time but exist in a fluid environment. The forces that work upon them vary in intensity and complexity. Among these forces are financial circumstances, personal problems, and work-related stress. Certainly not all of the forces affecting a person are negative, but those negative forces are the ones most likely to produce problems in the workplace

[1] Not her real name.

and are, therefore, of the greatest concern in worksites such as Janie's.

The DOE has developed a method to aid in assessing the current state of its employees and contractors who have direct access to Category I quantities of SNM. That method is embodied in the *Personnel Security Assurance Program* (PSAP). This assessment is focused on security concerns; in other words, only on those aspects of the individual that could potentially have a negative impact on the security of the United States. These concerns might be evinced through the failure to use sound judgment or to behave responsibly in the exercise of duties.

The elements of PSAP are fourfold: a supervisory review; a medical assessment; a management evaluation (which includes a review of drug test results); and a security review. The first three elements may be completed either within the contractor or the government system, depending upon whether the individual in question is a contractor employee or a DOE employee. The fourth element, the security review, is always conducted by the government.

(The DOE has a high ratio of contractor to federal employees in comparison to many other agencies. This goes back to the essential structuring of the Manhattan Project and the Atomic Energy Commission, when it was considered desirable to "civilianize" the atomic industry as far as possible. Most DOE nuclear sites are run by Management and Operating contractors as Government-Owned, Contractor-Operated entities.)

What does the implementation of the PSAP mean for Janie? In many ways there will be little noticeable change from the procedures and policies which now shape her life at work. The first element, the supervisory review, is an expansion of a process found in almost any job, whether this process is officially defined and codified or not. All employees are evaluated constantly: Are they doing the job? Are they working well with their peers? What is their potential in the company? The PSAP takes this evaluation process and adds one question: Is there any indication that the employee might pose a security concern? To be able to ask the question and to make an informed determination, supervisors of employees in positions covered by the PSAP will be given training in a number of topics. There is training about the PSAP itself, its purpose, design, implementation and desired impact; but also, and perhaps most importantly, training in the observation of unusual behavior. This latter type of training does not propose to make psychologists out of supervisors, but rather to give them guidance in what constitutes unusual behavior, when such behavior poses a security concern, and what steps, if any, should be taken. In Janie's case, the supervisory review portion of the PSAP means that her supervisor has attended training and that, on an annual basis, the supervisor signs a short form containing the statement that there are no security concerns about her. If such a concern should arise, it would be addressed at the time it is discerned.

Like the supervisory element, the medical element of the PSAP is an expansion of a process already present in DOE facilities. The DOE, through its contractor facilities, already has an extensive medical program that has historically concentrated on individual health and safety, as well as public health and epidemiology. At sites like Janie's, most workers are given a medical examination every other year. Those over 40 years of age receive an examination every year. Under the PSAP, all workers will receive an annual medical examination. The PSAP examination will be the same as the one currently given, with the addition of a psychological assessment. This assessment may take the form of a structured interview with the physician or a psychologist, aided by the use of standard test instruments such as the Minnesota Multiphasic Personality Index or the 16 Personality Factors. The PSAP medical examination is geared, like the supervisory review, to the detection of security concerns. Documentation is being developed to assist DOE and DOE contractor physicians with those aspects that may be a change from the standard DOE medical examination.

The third step in the PSAP process, the management review, brings together the previous elements, along with the results of an annual random drug test, and presents them for the review of a responsible management official. The drug testing process used meets the standards established by the National Institute on Drug Abuse (NIDA) of the Department of Health and Human Services. The drug testing is done through a urinalysis process with the samples being sent to a NIDA-approved laboratory. Should a test read positive for the presence of drugs, a confirmatory test is run on a reserve of the original sample. The results of the tests are sent to a medical review officer (MRO), who is an individual with expertise in analyzing and interpreting test results, and reviewed. In the case of confirmed positive tests, the MRO checks for possible explanations of the readings such as prescription drug use or some other biomedical reason.

Drug testing is not something new to the DOE contractor or federal population. Certain DOE contractors have had ongoing drug testing as a pre-employment requirement and as a follow-up action after an occurrence (accident) or when there is reasonable suspicion that an individual is under the influence of illegal drugs. Since 1988, DOE employees have been subject to drug testing under a DOE order derived from the Federal Drug-Free Workplace Act. All testing for illegal drugs is done in accordance with the "Department of Health and Human Services; Mandatory Guidelines for Drug Testing." DOE contractors may also test individuals in the PSAP for the presence of alcohol, following an incident or based on a reasonable suspicion of the individual being under the influence of alcohol.

For Janie the drug test provision means that during the course of the year she will be tested at least once. She may receive more than one test. The testing is not a true statistical random, as that would cause an unacceptable number of tests, and some individuals would be tested many times. Instead, a pseudo-random method is used which assures unpredictability as to the time of the test and prevents an individual or group of individuals from being singled out for testing.

The final element of PSAP is the security review. Every person selected for a PSAP position must possess a "Q" access authorization, the DOE personnel security clearance that allows access to restricted data and other classified information through the Top Secret level. This clearance is based on an initial background investigation, updated via a reinvestigation every five years. For individuals in PSAP positions there is, annually, a review of their security files, a review of an updated Questionnaire for Sensitive Positions, and a credit check.

And those, in brief, are the elements of the PSAP, none of them, in and of themselves, new to the Department of Energy or its contractors. But now these elements are being coordinated into a structured program that will assure equitable implementation and responsible oversight.

The complete PSAP cycle is conducted annually for all individuals in PSAP positions. If there are no concerns to report, a short form is annotated by all concerned in the review. If there should be a concern in any one of the four PSAP areas, it will be dealt with at the time it surfaces. The whole point of the program is to offer constant evaluation of the individual, as far as possible. When a concern is expressed, regardless of which topical element is involved, there is always the possibility of removing the individual temporarily from PSAP duties. Not all removals from PSAP duties have adverse implications for the individual. If, for example, Janie has a bad cold and is taking medication that affects her ability to do her job safely and reliably, she can ask to be temporarily reassigned until such time as she is capable of performing her tasks at the necessary high level of skill and accuracy.

One of the most important factors in the PSAP is not one of the four elements discussed so far, but is the training that goes with the program. This training has been prepared through the Center for Personnel Security Assurance, Research and Analysis, a division of Oak Ridge Associated Universities located at Oak Ridge, Tennessee. The training modules include a program to train security educators in the PSAP so that they may then train others at their sites, training for employees in PSAP positions and for their supervisors, seminars and workshops for those involved in the legal or medical aspects of the PSAP, and training in observing unusual behavior. For the PSAP to be a success, an informed and cooperative workforce is essential.

If the Personnel Security Assurance Program is a success it will benefit not only the Department of Energy but also the workers who participate in the program. The benefits for the DOE are obvious: a more secure site and decreased possibility of occurrences caused by impaired or unreliable workers. Those same benefits are enjoyed by those, like Janie, who go to work every day at these sites, and whose health, safety and job satisfaction are directly affected by the reliability of their fellow workers. ■

Lynn Gebrowsky is Security Specialist, Personnel Security Policy Branch, Policy Standards and Analysis Division, Department of Energy.

THE DENIAL OF FOIA REQUESTS FOR UNCLASSIFIED SECURITY VULNERABILITY ASSESSMENTS AND CLASSIFICATION GUIDES

Ronald W. Marshall

The Freedom of Information Act (FOIA) (5 U.S.C. 552, as amended), enacted into law in 1966, provides that individuals have a right to federal agency records, except for those records which are specifically exempted from disclosure under one or more of the following exemptions:

Exemption 1	Classified National Security Information
Exemption 2	Internal Personnel Rules and Practices (and other internal agency records)
Exemption 3	Records Specifically Exempted by Statute
Exemption 4	Trade Secrets/Commercial or Financial Information
Exemption 5	Internal Advice/Recommendations and Privileged Information/ Inspections
Exemption 6	Personnel and Medical Files
Exemption 7	Investigatory Information (for Law Enforcement Purposes)
Exemption 8	Financial Institution Information
Exemption 9	Geological/Geophysical Information

Among the FOIA requests denied to individuals by the government are those requesting the details of the security plans and procedures used to protect a government activity's assets against an external threat (whether that threat be from espionage or criminal mischief). Although very sensitive, because these security plans and procedures are rarely classified, they cannot be denied under Exemption 1.

Should a government agency receive a FOIA request for unclassified information of this sort, the agency's management is obliged, in the interests of the public at large, to consider denying it under Exemption 2.

FOIA denials under Exemption 2 are characterized as either "high 2" or "low 2." "Low 2" denials are those denials which are intended to relieve agencies of the administrative burden of assembling "matter in which the public could not reasonably be expected to have an interest"[1] and, typically, involve matters related to an agency's internal personnel rules and practices. What is interesting about the "low 2" exemption is that it is the only FOIA exemption that is not founded on harm resulting from disclosure: rather, it is based on the logic that denial is warranted because assembling this information (*i.e.*, information on routine and trivial internal agency matters) would cause an unacceptable administrative burden.[2&3]

However, what should be of interest to a government manager is the "high 2" exemption. In *Crooker v. BATF,* 670 F.2d 1051, 1074 (D.C. Cir. 1981), a major case involving a prison inmate's FOIA request for a Bureau of Alcohol, Tobacco and Firearms (BATF) training manual, the concept of the "high 2" exemption was firmly established. In that case the D.C. Circuit Court of Appeals opined that this exemption could protect internal agency records (not just internal *personnel* records) whenever their disclosure "significantly risks circumvention of agency regulations or statutes" or could "benefit those attempting to violate the law and avoid detection." Since this important case, reference is frequently made to the "dual" or "two-pronged test of *Crooker.*" The first test is the characterization of records as "predominantly internal" and the second, more difficult test, is whether or not the information "risks circumvention of agency regulations or statutes."

All Federal agencies are now required by law[4] to have security plans in place. These agency computer security plans appear to be ideally suited to denial under the "high 2," easily passing the dual-pronged test of *Crooker*. First, the plans deal with a computer system used only within the agency by agency personnel. Second, the plans describe, in detail, the most vulnerable portions of that agency's computer system and must further outline the security measures that have been taken to protect the system's integrity.[5] Information of this sort could allow an individual to penetrate an agency's computer system, conceivably destroying valuable records or rendering the system unusable. Logically, then, a significant risk of circumventing a statute (i.e., the Computer Security Act) exists. Recent case law has upheld the legitimacy of this rationale.[6]

Similarly, a case was made for the denial of unclassified security classification guides under the "high 2" exemption in *Institute for Policy Studies v. Department of the Air Force*, 676 F. Supp. 3, 5 (D.D.C. 1987). Security classification guides are documents which assist agency personnel in properly classifying national security information and are intended for internal use only within the Executive Branch.[7] Their unimpeded release could allow persons or foreign governments to identify the most sensitive parts of classified U.S. government programs and engineer collection efforts against them (and, therefore, conceivably "circumvent" the Espionage Statute [18 U.S.C 794-8]). However, a compelling argument for their release is that if these security classification guides are that sensitive, why aren't they classified (and hence covered under Exemption 1)? The logical answer is that just like computer security assessments (which are typically unclassified) this information is administrative in nature and requires fairly wide distribution to agency users. Classifying this information would severely limit its effectiveness by limiting its dissemination. Nonetheless, there is a very tangible possibility that damage might occur if the information was maliciously or illegally used.[8]

Aside from its immediate significance as a landmark "high 2" FOIA case, the *Institute* case was significant in that it rebutted the plaintiff's contention that the government was attempting to use an "anemic" form of classification. The plaintiff further contended that this ran counter to Congressional intent in the FOIA to protect only that national security information properly classified under Executive Order 12356. The Court did not agree and found instead that "the use of Exemption 2 to withhold internal agency information on grounds of national security is not inconsistent with Exemption 1," and, further, that "there is considerable overlap among the FOIA exemptions."

This assertion by the court of the existence of unclassified national security information is quite provocative. Executive Order 12356 of April 2, 1982, National Security Information Sec. 6.1 defines national security information as information that has been determined pursuant to this order or any other predecessor order to require protection against unauthorized disclosure and that is so designated. The "protection" afforded is protection through classification. Therefore it follows logically that if government information is not classified it is, by definition, not national security information. Whether the court understood the ramifications of recognizing the existence of "unclassified national security information" is moot. It saw, from a practical perspective, that the requested information was sensitive and the government's attempt to deny it was legitimate and in the public interest.

In the coming years, as FOIA case law matures, the "high 2" exemption may yet prove to be the government's most useful mechanism for protecting information that falls into the slippery, and ill-defined, category of "unclassified national security information."

References:

[1] *Department of the Air Force v. Rose,* 425 U.S. 352 (1976).

[2] *Protecting Vulnerability Assessments Through Application of Exemption Two*. FOIA Update (U.S. Department of Justice) Summer 1989. While this article specifically speaks to security assessments it is stated that such an assessment commonly will describe the *specific security measures* (as well as possible countermeasures) that can be employed to combat the vulnerability. (emphasis added).

[3] *Rose* and *Institute* undermine other court's contentions (see *Jordan v. Department of Justice,*

591 F.2d 753, 767 [D.C. Cir. 1978] and *Allen v. CIA*, 636 F. 2nd 1287 [D.C. Circuit 1980]) that the intent of Exemption 2 is narrowly focused on personnel records.

[4] Computer Security Act of 1987, Pub. L. No. 100-235, 101 Stat. 1724 (1988).

[5] DOJ, *FOIA Update*, (4).

[6] See *Oliva v. Department of Justice*, Civil No. 84-5741 (S.D.N.Y.), *Wightman v. BAFT*, 755 F. 2d 979, 982 (1st Cir. 1985) and *Hall v. Department of Justice*, Civil No. 87-0474 (D.D.C 1989).

[7] The classification of information has been an Executive Branch prerogative since the 1790s. In 1973, the 93rd Congress (specifically the subcommittee of the House Committee on Government Operations) in hearings on H.R. 12004, attempted, unsuccessfully, to amend the FOIA to provide for the "classification and declassification of official information in the national defense." This would have created a statutory basis for the classification of national security information.

[8]Many security classification guides are considered technical documents and have distribution statements to that effect. These guides should be withheld under Exemption 3, which protects from disclosure information specifically protected by statute. The statute in this case is 10 U.S.C. 130, which contains authority to withhold from public disclosure unclassified technical data with military or space application.

[9]The Institute for Policy Studies FOIA request was for a security classification guide for the Air Forces Ground Wave Emergency Network (GWEN). The GWEN is a radio network that is designed to ensure the connectivity of government communications during and after a nuclear attack. The guide specifies which GWEN information is classified, at what level it should be classified and when it should be declassified. ■

Ronald W. Marshall is RANKIN Program Manager for Security Classification Guides, Department of the Navy.

DETERMINING THE EFFECTIVENESS OF SECURITY AWARENESS PROGRAMS

Peg Fiehtner

Experienced security professionals are tempted to presume that everyone with a security clearance knows the basics of security. This is a dangerous presumption. It is particularly true for those with SCI[1] access. How many people could give you a correct explanation of the difference between a classified document containing collateral information and one that contains SCI? You might be surprised at the results! We need to appreciate what our people DO NOT know, or what they once knew and have since forgotten.

When challenged about safeguarding and storage standards, most people turn to the regulations and cite the minimum requirements. The minimum may not be good enough. Standards must be determined for each site.

The security manager preparing an awareness program should consider the unique features of each location that deserve coverage in a security briefing. For example, the U.S. Navy regulation requires that everyone with access to classified information must have a counterintelligence (CI) briefing every two years. The Naval Security Group Command Headquarters is located in the heart of the embassy district in Washington, D.C. A CI briefing every two years is not often enough.

A security manager can assess the effectiveness of the organization's awareness program systematically and methodically by defining:

WHAT are we protecting?

WHO is protecting it?

WHAT is the threat?

HOW well is that threat being countered?

Consider the scope of your mission and the extent of sensitive or classified information under development or in custody.

How many people are cleared? How many have access to SCI? To collateral? To SAPs? How many do not have access and should they be part of your security awareness program? Scope is an important aspect of an awareness program.

What is the threat? What is the source of that threat? What are the internal vulnerabilities? How much does the cleared populace know about the threat and how well educated are they to counter it?

And, how do you gauge how well that threat is being countered?

Your source of this information should be a threat assessment conducted by a counterintelligence unit. You need an analysis of your internal security violations and discrepancies and an identification of trends. Do you conduct liaison with investigative elements? What about quality control reviews and results of external inspections and oversight visits? Determine the extent of classified material and information held and developed (*i.e.*, take inventory). Perhaps most critical to the program: get feedback from your cleared people.

Do you manage the security violation program? If so, this is an extremely important area to monitor because it will provide the strongest indication of weakness and tell where you need to target training or awareness. If you do not manage the program, find out who does and get feedback. Contact higher authority or other security managers in the region and find out what they are experiencing. Are your violations the same as others, or are yours unique? Conduct an analysis. Do violations occur because people are negligent, or ill-informed? Do they occur because the proce-

[1] Sensitive Compartmented Information

dure or system is at fault? How often do they occur? Is a trend developing?

Establishing trends provides fodder for "preventive maintenance." A series of minor deficiencies, for example, is a violation waiting to happen. You won't even see trends if you aren't aware of the specific events. Conversely, a lessening of deficiencies may also show a trend which implies that training of enhanced awareness is working, and other problems can be brought into focus.

You also need information regarding current threats, whether from hostile intelligence services, indigenous terrorist cells, or criminal activity. Sources of this information range from local law enforcement agencies and the FBI to military counterintelligence organizations and American Embassies overseas. You cannot effectively counter the threat unless you clearly define what it is.

The bottom line is how well are you countering the threat? Inspection results, quality control reviews, and feedback from cleared people are but a few of the tools at our disposal. Inspection results from an IG or any other "external" source provide written estimates of the strengths and weaknesses regarding your program. Do you receive these results? Quality control reviews are generally conducted by the internal security staff. Some are scheduled within each element and are rather formal, while others may be little more than a casual walk through of spaces by an observant security professional.

Talk to your people. Get their reactions, impressions, recommendations and complaints. Are their attitudes positive? Resentful? Supportive? Cavalier? Do they have specific desires, interests or questions regarding security? Are they cooperative and conversant? Do they view the security staff as part of the team or as individuals "out to get" someone breaking the rules? If the only time you leave your office is to investigate a violation or wrong doing, you have established a negative impression. Your people will not be willing to talk to you or your staff and a vital link will be broken. Negative attitudes toward security reduce the effectiveness of your program.

Some examples of assessment projects that have worked within the Federal Government include:

A **multiple choice quiz** (non-attributable to the individual) which queries a variety of security procedures and policies. The quiz is completed at the convenience of each person and is returned to the security office. Inquire whether the individual wants it returned when "graded." The purpose is not to target the individual, but rather to accumulate data regarding the amount of correct and incorrect answers. You will know which areas need attention and, just as important, those that do not.

Questionnaires provided to a target audience. They solicit information and impressions regarding local security practices and procedures and request security briefings they would be most interested in receiving. The key to success here is the method of distribution used. While the questionnaire is drafted by the security staff, it is "smoothed," signed, and delivered by the section or department head. The surprise from this method was the 98% response rate of completed questionnaires.

"Man on the Street" interviews. Do you have a local newspaper or security newsletter? Everyone likes to see their name in print. Select some good topics (you needn't shy away from the controversial), and conduct quick, random interviews. Get their input and impressions. Publish the results. Pictures, too, if that can be accommodated. This method provides tangible evidence of community involvement and interest in security and also gives security an opportunity to ask questions in a positive environment.

A close relative of interviews is a **standing display** of photographs of individuals performing security functions: securing a container, completing a security form, sealing a burnbag, locking a vault. Displays of this nature will draw a crowd, particularly if you inform the individuals in advance that they may keep the picture when the display is removed. Be prepared for those who will want to know why THEY were not asked to participate:

Security Teams. Larger organizations have established security points of contact in various work spaces for department to act as liaison with the Security Staff. These individuals are deliberately NOT security professionals. If you are aware of a negative attitude toward the Security Office and wish to take some initial steps to overcome the reputation, this method is a good start. Essentially, security teams establish a buffer system between your office and the cleared populace. The person acting as a buffer is "one of their own." Meet occasionally with these points of contact and provide some interesting, pertinent, positive information on the organization's security posture and concerns. Show them "what's in it for them." This is part of the marketing security concept.

These assessment projects certainly do not constitute the best or only methods of assessing the effectiveness of a security awareness program. But these methods have worked and, perhaps, will form the basis for other innovative projects. ■

Peg Fiehtner is Deputy Special Assistant for Security, Naval Security Group Command.

NISP: Assessing Today's Security Reality and Recreating a Vision for the Future

Maynard C. Anderson

"There is nothing more difficult to take in hand, more perilous to conduct, than to take a lead in the introduction of the new order of things, because the innovation has for enemies all of those who have done well under the old conditions and lukewarm defenders in those who may do well under the new."

Niccolo Machiavelli, 1532

Bill DeGenaro, who was the Director of Innovation Resources for the 3M Corporation, came to the Department of Defense in 1989 through the President's Commission on Executive Exchange. He worked that year as my Director for Strategic Countermeasures Planning.

Bill likes to talk about frogs. He recalls that anthropologist Gregory Batesman, a long-time student of both frogs and men, has pointed out the marvelous capacity of our web-footed friends. Different species of frogs are found thriving from the steamiest jungles to the sub-Arctic, where they survive winters in a kind of suspended animation. According to Batesman, if a frog in suspended animation is thrown into a pot of hot water, it will instantly sense the temperature and leap out. However, if the frog is placed in room-temperature water that is gradually brought to a boil, the frog is incapable of sensing the change, and it will boil to death.

I tell you this story to alert you to the possible consequences of incremental changes all around us. The frog broth is slowly heating up, forcing a proactive, not a reactive, stance toward the future. Innovation represents our best and possibly our only hope for extricating ourselves from what could prove to be a very bitter soup.

Noel Tichy, one of the country's leading organization experts, says this about the beginning and most important step of the process of change.

"Perhaps the most essential component of a transformation is a vision of the future desired state. Transformations require a dream and require the organization to aspire to be something. Yet, some way of assessing the current reality is also required in order to determine whether the vision fits with reality."

So, the critical beginning point is establishing a vision, which must be based on some notion of utility. Defining the activity helps determine the utility and establish the boundaries within which we need to perform. There is a necessary creative tension that develops in the gap between vision and current reality.

We are always faced with a situation of tradition v. innovation. (Some would say we are also always faced with a situation of policy v. reality.) It is in the context of both of these contests that things like a National Industrial Security Program (NISP) develop.

We are present at the moment of recreation, to paraphrase Dean Acheson.

In the recent past, we haven't given much thought to what we really mean when we say "National Security," probably because there was a fairly stable threat situation. There was an easily identifiable and well-defined enemy.

"The full implications of the dramatic reduction of the threat that was for forty years the polestar of american security policy are still being assessed. Even to talk of "threats" now smacks of the past age of the cold war. But while everything can be a challenge, not everything is a threat."

(Final report of the seventy-ninth American assembly on "rethinking America's security," Council of Foreign Relations,Inc., 2 June 1991.)

The traditional view has now given way to consideration of something that we might call the "national interest." For example, we have always dealt with national security information in the traditional sense of its definition as "classified information." It requires protection. We must also now deal with technology, not always classified, but described as "unclassified, sensitive, national security-related information." An amorphous body of material, it requires various kinds of protection. And, more and more, these kinds of information are in the hands of multinational corporations, or United States companies operating under some degree of foreign ownership, control or influence. There is the threat of economic espionage, something we haven't really thought about defining let alone combatting. But, new challenges and few resources force us to do both with creativity and innovation. And, the "National Security" is certainly part of the national interest, or, is it the other way around in these new times?

We are now being compelled to determine the possible threat against each of a number of core technologies--five to ten years in the future. That requires that we direct our energies against kinds of dangers, or threats, as opposed simply to specific geographical entities or political organizations that are their proponents. This has resulted in the recognition that there are both states and issues to be confronted. Communication of both the threats and the value of what must be protected to our decision makers on a continuous basis is going to be one of our necessary objectives.

The threat, which demands definition continuously, has enlarged geographically and changed politically as well as economically. But, the threat is not always the determinant for protection. Sometimes, we must look at whether something has value. Is it worth protecting? If so, protection is against the generic threat of loss. The protective systems we apply then are somewhat analogous to buying an insurance policy.

"Value" means an assessment of real worth. "Damage," the traditional measure of the need for protection in our system, is a postulated assessment of diminished or lost capability.

The value of information is its contribution to its intended or specific purpose--ensuring the national interest, protecting the national security.

We are beginning to construct an entity in the form of the NISP that will allow us to focus both our efforts and our resources on information that is truly in need of protection that is going to be in the hands of industry.

As a predication, review and revision of E.O. 12356 provides an opportunity to fix some things that might continue to cause us problems. One of the things that has caused us problems, and, in fact, has contributed to the need for the creation of a NISP, was the proliferation of special access programs (SAPs).

To create a SAP, it must be shown specifically that normal security measures are inadequate. One might argue that to impose more extensive security requirements, along with more restrictive information handling controls, is equivalent to establishing a classification higher than Top Secret. I don't believe that is the intent of the executive order.

I have argued that a SAP should be created only under the presumption that an individual's life or safety would be endangered, or that national security would be substantially and irreparably jeopardized by releasing the information into the public domain. SAP controls should be limited to the handling, dissemination, and declassification of information. There should be no additional personnel security investigative requirements and there should be a single adjudicative process.

Those arguments served to stir the frog broth. Along with other arguments that program managers did not need to classify everything that surrounded their program's activities, that there should be challenges to classification when it was clearly questionable, and that protection applied should be based on analysis and evaluation fo the environments in which we operate, the cauldron came near to boiling over.

Because of the predominance of the defense industrial security program (DISP) in classified contracting, the Department of Defense is clearly responsible for many of the actions that led to the concept of a NISP.

During the '80s, there was a great deal of controversy swirling about industrial security. At every meeting of the Aerospace Industries Association (AIA), the American Society for Industrial Security (ASIS), the National Classification Management Society (NCMS), the National Security Industrial Association (NSIA), and all of the other organizations (ADPA, AFCEA), there was a discussion in the formal program of the relationships between contractors engaged in classified contracting and the government. The "Government" in this case generally meant the Department of Defense.

There was talk about a "partnership," and "equal treatment," and how to accommodate all of the different requirements of various programs that began to emerge, first in the intelligence community and then in the world of acquisition.

The Director of Central Intelligence is the proponent for intelligence programs on the national scale, of course, both in accordance with E.O. 12356 and the National Security Act. The intelligence programs, generally, did not cause a great deal of trouble in terms of industrial contracting.

Overlaps began to occur, however, as certain programs began to grow. We refer euphemistically to the "specialized reconnaissance programs of the DoD." All of those began to require extraordinary industrial contracting support. They were organized, however, and operating efficiently for the most part.

There was some "creative tension" between the intelligence world and the "regular" security world (this may have been the first gap between vision and reality.). But, it was not the major area of contention between contractor and government.

During the '70s and '80s, there began to emerge a spectre that frightened the administrator of the Defense Industrial Security Program (DISP).

The *DISP*, created by executive order 10865, following the Supreme Court's *Green v. McElroy* decision, allowed the Secretary of Defense to operate his own industrial security apparatus, as well as make it available to any other department or agency through an exchange of letters. Today, more than 20 other federal organizations, to include the general accounting office, take advantage of that support. What began to emerge that caused the *DISP* concern were numerous special access programs protecting weapon systems acquisition, many of which had diverse requirements, and which were "carved-out" from inspection by the Defense Investigative Service (DIS), the administrator of the *DISP*.

The "SAPs" and "carve-out" contracts caused a number of problems. Those that were begun by renegade program managers in the belief that they allowed more efficient operations were imposing costly requirements on the contractors involved.

They also hid from view possible security irregularities that would have been disclosed through regular *DISP* inspections. In all fairness, there were some structured programs that controlled advanced technologies used to produce modern, sophisticated weapon systems that were of much benefit to the government. There were many, however, that were of questionable value and appeared to be nothing more than a means to circumvent proper inspections and sometimes proper management.

In counterpoint, the DIS administration of the program had become so structured, rigid and inflexible in so many ways that many program managers sought relief in provisions that allowed exemption from the DISP.

Thus, there emerged not only controversy between industry and government but controversy between various components of the Department of Defense as to the best way to ensure industrial security. Occasionally, the intelligence community, the Department of Energy, and the Congress became embroiled in the controversies as well.

Special access programs came under intense scrutiny and the DoD strengthened the management, control, and oversight of those programs through establishment of a stronger regulatory base and a set of somewhat more practical standards for establishment.

Some concerns were satisfied, but many elements of both industry and government remained dissatisfied. There were still reports of large numbers of inspectors visiting the same facilities to look at the same things, and levying "ad hoc" and sometimes whimsical requirements on their hosts. As a result, large amounts of money were spent to build unnecessary facilities, investigate personnel for high clearances and accesses that were questionable, and control information that was classified beyond its actual sensitivity.

There emerged an evolutionary recognition that there must be some kind of movement toward a *rational* industrial security program.

The *NISP* concept began in 1988 when it was recognized that there were more than 1.5 million cleared contractor personnel working in more than

15,000 cleared facilities (3,000 of which also housed SCI[1] or Special Access Programs); and, there were a variety of rules, regulations, and instructions all designed to protect the same or similar kinds of material in these facilities. Subsequently, it was determined from survey cost data provided by the Aerospace Industries Association that total estimated program cost to the government for the year 1989 was $13.8 billion.

Industry and government recognized that more centralized national planning and direction could play a key role in improvement of security in industry. Concept planning concentrated on improving the administration of the program and ensuring security cost-effectiveness; establishing security standards and procedures applicable to all; and providing continuing evaluation of personnel to assist in the early detection of espionage.

On 4 April 1990, the president directed a national security review of the government's industrial security programs to determine the feasibility of establishing a single program, applicable to all government departments and agencies.

In November 1990, a response to the president advised that the Secretary of Defense, the Secretary of Energy, and the Director of Central Intelligence supported the concept of a NISP and would work together, with industry representatives, to: (1) conduct a zero-based regulatory review; (2) develop an instrument of authority; (3) develop and promulgate standardized security policy; (4) establish a mechanism for determining industrial security costs; and, (5) ensure completion of ongoing personnel security initiatives for a single-scope background investigation. On 6 December 1990, the president concurred and directed that a report on recommended policy changes be provided to the National Security Council by 1 September 1991.

Following the president's concurrence with the feasibility determination, a NISP task force was established. Today, eight departments or agencies as well as industry are represented on the steering group and there have been 11 working groups and sub-groups in which 170 representative of government along with 85 industry representatives worked to meet the deadline of providing the National Security Council with a report.

The report to the National Security Council outlines accomplishments, issues yet to be resolved, work yet to be done, a recommendation for action by the president and a "critical path" for full implementation of the NISP.

It is anticipated that a revised E.O. 12356 will include the authority to protect national security information both in the hands of government and industry. The policy implementers will be in the form of information security oversight office (ISOO) directives, and the procedural implementers will be in the form of a NISP operation manual (NISPOM). The ISOO might well be the oversight organization, ensuring that classified information is properly protected in industry as it does now in government agencies.

Physical security base lines are being constructed for the protection of all kinds of material. There will be a revised DCID 1/21 (standards for sensitive compartmented information facilities) and simplified standards for SAPs (hopefully, only one level between regular material and SCI.).

Reciprocity of inspections will be ensured through negotiation of memoranda of understanding among affected cognizant agencies.

A single scope background investigation (SSBI) has been devised for access to both Top Secret and SCI.* A uniform personnel security questionnaire is scheduled for completion in January 1992; standardized adjudication criteria are scheduled for completion in June 1992; and reciprocal acceptance of all clearances anticipated by June 1993. Common administrative review procedures for personnel holding both regular clearances and SCI accesses have been agreed by the working group.

In addition to concern about the administrative aspects of investigations, adjudication (DMRD-986), and due process, personnel security is also a study of how to determine vulnerabilities both of positions and people. We are trying to find better ways to continuously evaluate our cleared people; to improve the means to determine financial anomalies that might indicate improper activities; to determine forensic means that might lend credence to suspicions of improper behavior; to

[1] Sensitve Compartmented Information

**On 21 October 1991, President Bush approved the Single Scope Background Investigtion by issuing a National Security Directive.*

improve the polygraph so that its use will be less intrusive, produce better results with greater reliability and more validity. We are looking for ways to grant clearances without relying on background investigations.

Perhaps not long from now, as we walk into a facility, our "aura" will advise the control officer that we are eligible for access. We are born eligible for access (even taking into account the concept of original sin). We might think about a future system that will allow access unless there are apparent reasons for ineligibility. Is this adjudication by exception? Not if we maintain a record of our accountability that also meets the test of providing proper protection of privacy.

In the midst of all this procedural change, concern for people is what remains constant. We need to ensure through every means possible that we do not fail them in providing leadership and opportunities for them to improve in the process of change.

One of the opportunities available in the NISP is an academic initiative. The DoD, Michigan State University, and industry, have undertaken development of a program of instruction and research at the graduate and undergraduate levels with emphasis on the NISP. In addition to degree programs in security management, the university will provide security professionals with advanced study and research opportunities through creation of a center for security leadership and management.

Jointly funded by government, the university, and industry, the program also provides for creation of a computer laboratory and a security resource library to augment existing university resources. This program will enhance all professional aspects of every security discipline as well as contribute to more informed policy decision through rigorous research and study.

It is obvious that the NISP will probably be a catalyst for significant changes in how the government does business in security in the future. It will produce major cultural changes in information security, physical security, personnel security, and international security which will have great impact on how those disciplines are implemented in any circumstances.

From the perspective of counterintelligence and security countermeasures, the world of our concerns has suddenly become too small. The well-defined enemy has dissolved into a kaleidoscope of potentially harmful adversaries and friends.

On an international scale, there can be no doubt that we will be assaulted, if not taken advantage of, by foreign competitors; not hostile nations, but foreign nations.

We must reorient our constituencies to understand that there is no longer merely a hostile threat, but whatever it is that we decide has value must be protected from unauthorized disclosure.

That which we want to protect must be clearly identified. Discriminating classification should produce less classified information, but we will probably have to protect more information in the form of technology and economic data because they are factors in U.S. economic competitiveness. It is still our objective to control certain technologies while attempting to ensure the competitive position of U.S. industry in the world market.

Security systems have failed to prevent espionage. I suspect that it is because their character and their application have not engendered the respect of both those who are subject to the systems and those who apply them.

I believe the best way to translate our vision into utility is to make sure that our cleared population participates in the process of counterintelligence and security on a daily basis.

There are those who will tell you that a NISP won't work. It won't work if we don't make it work.

You share a responsibility to your respective organizations and your government to try by taking this first step of progress. We need to think less about ourselves and more about our circumstances or we will not perform this responsibility as we should.

Is everything perfect, and properly done at this stage? Probably not. Have we made mistakes? Probably.

Cooperation is the greatest asset within society. It will produce a better program.

I encourage you to participate--to join in this process of recreation that we call the NISP.

"What you can do, or dream you can, begin it."
"Boldness has genius, power and magic in it."

Goethe

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

LIMITED DISSEMINATION CONTROLS ARE NOT SPECIAL ACCESS PROGRAMS

Raymond P. Schmidt

This article highlights what Limited Dissemination controls add to our standard system of security protection for classified data and information. It compares them with Special Access Programs because the two are often mistakenly perceived to require the same or comparable security measures.

Introduction

The SAP, or *Special Access Program*, has played a special role in the Department of Defense (DoD) information security program for many years. As will be explained in more detail, SAPs have an identity all their own because they impose security requirements beyond those of the normal security system.

On the other hand, LIMDIS controls, which stands for *Limited Dissemination controls*, are an integral part of the standard security program. Once SAPs and LIMDIS controls are explained and their characteristics compared side by side, no security professional can confuse the two.

In general, security specialists should know that SAPs and LIMDIS controls do have several superficial similarities, but they are significantly different in their main characteristics. SAPs and LIMDIS controls are alike in that they both limit the need-to-know, and they employ distinctive markings that set the protected data and information apart from other National Security Information (NSI).

Both can serve security requirements of program managers--much as tanks and cars both serve basic transportation needs. But, just as tanks and cards afford varying levels of protection to those riding inside, SAPs and LIMDIS controls differ greatly in how they accomplish the task of affording protection to the classified information that they "surround."

LIMDIS Controls

Several years ago, the Deputy Under Secretary of Defense for Security Policy authorized use of the distinctive new LIMDIS control measure, which employs existing restrictions stated in the general DoD regulations to help protect specified NSI. Simply put, *LIMDIS controls* implement the need-to-know security principle in a formal way within the *normal* security program.

The Department of the Navy (DON) applies LIMDIS controls only to classified data and information that have been identified in an approved security classification guide. The Top Secret original classification authority responsible for developing that guide must confirm in writing the compelling need to employ LIMDIS controls, and request assignment of a nickname. The approval process also requires coordination with the Department of the Navy office having cognizance over SAPs to ensure consistency. LIMDIS controls are approved by the Assistant for Security Policy (OP-09N2) in the Office of the Special Assistant for Investigative Matters and Security. The approval is given for a specified period of time, normally two years, and must be justified again to be extended. No other LIMDIS controls may be imposed by any DON official.

Once formally activated, LIMDIS controls are implemented and administered through the security manager for each command or staff element. A brief plan explaining how to administer them may be developed, and must be approved by OP-09N2 in the same manner as is the security classification guide. The plan may explain how the LIMDIS two-word nickname is used to identify the classified data and information involved; it may repeat general DoD and DON regulatory requirements for marking documents and inner wrappers; and the plan may restate the normal procedures for transporting, transmitting, and storing LIMDIS controlled material.

The only special physical security restriction employed is to place LIMDIS material in sealed envelopes within approved storage containers to avoid inadvertent disclosure or comingling with other files. Security specialists will recognize a similarity in this respect to the procedures for handling NATO material.

Inner envelopes containing LIMDIS material are marked "TO BE OPENED ONLY BY PERSONNEL AUTHORIZED LIMDIS LIMIT (SECOND WORD) ACCESS" but with no other unique markings.

Electrically transmitted messages carrying LIMDIS data or information may be marked with the uniform caveat "LIMDIS LIMIT (SECOND WORD)."

All of these procedures are authorized by the Department of the Navy Information and Personnel Security Program Regulation, or by the Department of Defense Industrial Security Manual for contractors. Nothing in the LIMDIS plan even suggests *special* security measures are authorized for clearances or for handling, transmitting, or storing LIMDIS controlled material. This is quite different from a special access program.

The LIMDIS plan also provides a briefing acknowledgment statement to be signed by those for whom a need-to-know the LIMDIS controlled data or information has been determined. Each individual granted access signs a statement which is retained by the local security manager.

In this manner LIMDIS controls provide enhanced observance of the need-to-know principle. Most importantly, there are clearly strict boundaries to such controls. Note: LIMDIS *programs* do *not* exist, only LIMDIS controls applied to specified classified information or data *within* a program or project.

SAPs

Security specialists who work with SAPs already understand how the formal rules for them operate outside the standard U.S. scheme of information, personnel, and physical security. For those professionals who do not, a brief explanation will give you an adequate background for purposes of comparison.

SAPs are centrally-managed security *programs* established by designated agency heads under Section 4.2 of Executive Order 12356 as implemented by Information Security Oversight Office Directive No. 1.

Many of the largest programs reside within the DoD, and are governed by special DoD regulations. Recent changes to DoD policy further strengthened the previous tight constraints on their approval and management. Any one of four senior DoD officials can approve a SAP, but only if they have prior written authorization for it from the Secretary or Deputy Secretary of Defense. Such programs must meet two formal criteria:

- Normal management and safeguarding procedures do not limit access sufficiently to protect classified NSI; and

- The number of persons who are granted access is limited to the minimum necessary to meet the objective of providing *extra protection* for all information in the program.

The *extra protection* comes from additional investigative or adjudicative procedures for persons seeking access; specially designated officials who are authorized to determine whether cleared personnel have a need-to-know; central lists of persons who are authorized access; use of codewords to identify information requiring protection; unique written security regulations and procedures; specialized funding, contracting, and logistics procedures; and dedicated oversight and frequent inspections.

Information in SAPs is almost always identified by markings which state that it has "SPECIAL ACCESS REQUIREMENTS" or that otherwise reflect its status as part of a special access program. These markings place the viewer on notice that exceptional security procedures govern its handling, storage, transmission, transportation, and disposal.

Thus, SAPs are security programs with a formal administrative structure designed to *control access* to and *restrict distribution* of classified information about that program. They are subject to

Characteristics that Distinguish Between LIMDIS Controls and SAPS

Characteristic	LIMDIS Controls	SAPS
Authorization	Determined by Agency Head (Navy: OP-09N2)	SECDEF/Deputy (in writing)
Access Determination	Local Command/Facility by Need-to-Know	Central Billet Control
Personnel Orientation	Briefing	Indoctrination
Record of Access	Signed Acknowledgement Statement	Sign Legal Oath
Retention of Record	Local Command/Facility ONLY	Centralized by SAP Program Manager
Termination of Access	Remove from Local Command/Facility Access List	Sign Formal Debriefing Oath
Termination of Program	None (Advise holders of Termination)	Reported to Congress
Marking	Identified by Unclassified Nickname (only)	Identified by Codeword
Physical Security	Standard (Notice on Inner Wrapper)	Special (As Prescribed)

Figure 1

high level management attention, tight central management, and special oversight.

Comparison of LIMDIS Controls with SAPs

Further discussion of security requirements and a side-by-side comparison of LIMDIS controls and SAPs will help in reviewing what has just been outlined. *Figure 1* depicts key characteristics for ease of reference.

First, why do program managers appear to require SAPs or LIMDIS controls at all?

To answer this question, we must consider the *procedures* for deciding whether personnel are eligible for security clearances: Granting a member access to classified information is preceded by an official determination that a person is reliable, trustworthy, and loyal to the United States. This involves several steps:

- A responsible official decides that a position requires the incumbent to handle classified information of a specified level.

- Next, a personnel security investigation is completed so that the request for clearance can be adjudicated and a security clearance issued.

- When the record of clearance is received by the requesting official, the appropriate security manager gives an initial security briefing to the incumbent. This is intended to ensure that he/she understands and agrees to comply with security regulations and the sanctions for violating them.

- Then, and only then, should the command or company grant the individual access to classified information.

Even at that point, however, the eligible member should not see, hear, or use classified information until he/she has a valid NEED-TO-KNOW it. That need must be demonstrated to the satisfaction of the official who already has authorized possession, knowledge, or control of that information.

The need-to-know decision is made by *each* official who possesses or controls classified information, not by the person seeking to know it.

At this point, it may be helpful to recall what the need-to-know principle says:

Access to, knowledge, or possession of classified U.S. National Security Information (NSI) is limited to those personnel possessing a security clearance who require NSI to perform a specific and authorized national security task or service in the fulfillment of an official United States government program.

Executive Order 12356 emphasizes that such access must be essential to accomplish "lawful and authorized Government purposes." Note the similar emphasis in the quoted definition on *specific* and *authorized* tasks. Experienced civilian and military members of the Government and industry realize that knowledge of classified information places a burden on them which ends only upon its formal declassification. They avoid acquiring more classified information than they need to do their jobs. This provides an opening to mention a corollary security principle:

No one has a right to have access to classified information solely because of rank, position, or security clearance.

Every U.S. citizen with a security clearance should understand and use the need-to-know principle. If it always worked perfectly, no other access and handling controls would be needed. Obviously, however, experience demonstrates that additional measures must be taken to protect classified information of a particularly sensitive nature.

Therefore, in the context of imperfect application of the need-to-know principle, some program managers can effectively argue that they need SAPs or LIMDIS controls to ensure adequate protection for this information. Part of that protection derives from the reassurance that both require interviews with cleared personnel to ensure that they have a valid and certified need-to-know to obtain access to specified National Security Information.

Second, how do SAPs and LIMDIS controls apply the need-to-know principle, and how do they differ?

Note the characteristics of SAPs and LIMDIS controls:

SAPs: Some National Security Information deserves such a high degree of protection that programs which *supplement normal security requirements* have been devised to help program managers safeguard information in the SAP.

A SAP usually imposes written special and formal safeguards for controlling documents and granting personnel access that are more stringent than those stated in general security regulations. These safeguards may include the use of codewords and nicknames to highlight the classified information deserving tight protection, investigative or adjudicative requirements for SAP personnel, special security briefings and indoctrination agreements for those given access, centralized listings of personnel authorized access to the SAP information, and extraordinary storage and handling procedures for classified material unique to the SAP.

SAPs are identified exclusively to those who have a need-to-know and are indoctrinated into them. Access by any individual to a specific SAP is often decided by a central authority and is subject to a rigidly administered billet structure.

LIMDIS controls: Other NSI that does not meet the criteria for SAP protection still requires additional enhancements to ensure enforcement of the need-to-know. LIMDIS controls are administered as part of the *regular security system*--not as a separate program, as in a SAP.

LIMDIS controls are intended to establish simple formal procedures that restrict personnel access to specified NSI. The security manager administers these procedures.

Unlike the case with SAPs, no special investigative or adjudicative requirements may be imposed. A briefing covering the LIMDIS plan and security classification guide is provided to those allowed access to the controlled information, and

Comparison of Limdis Controls and SAPS

Question	LIMDIS Controls	SAPS*
Implement the need-to-know principle?	Yes	Yes
Serve security requirements of program managers?	Yes	Yes
Distinctive markings?	Yes	Yes
Standard security requirements?	Yes	No
Unique security regulations and procedures	No	Yes
Special access requirements?	No	Yes
Central management?	No	Yes
Additional investigative procedures?	No	Yes
Additional adjudicative procedures?	No	Yes
Special funding arrangements?	No	Yes
Special contracting procedures?	No	Yes
Special logistics procedures?	No	Yes
Dedicated oversight?	No	Yes
Frequent inspections?	No	Yes
Signed indoctrination oath?	No	Yes
Signed briefing acknowledgement?	Yes	No
Central billet control?	No	Yes
Central lists of people granted access?	No	Yes
Dedicated transmission channels?	No	Yes
Dedicated transportation channels?	No	Yes

*It should be noted that not all SAPs have all these features. They adopt only those features essential for that program.

Figure 2

each individual may sign a briefing acknowledgement statement. Each command or company is required to retain the list of personnel briefed, but centralized listings are not permitted (*i.e.*, no quota management or billet structure).

Unclassified nicknames, not code words, are used to identify the elements of information that require formal need-to-know access approval. No special physical security measures may be employed, except to place LIMDIS material in sealed envelopes within approved storage containers to avoid inadvertent disclosure or comingling with other files.

Generally, LIMDIS controls operate only inside the agency that created them, whereas SAPs often cross agency lines. LIMDIS controls are normally approved only for specified brief periods of time, whereas SAPs may have indefinite life spans.

Finally, note that LIMDIS controls are the *only* security enhancement short of a SAP that may be employed for control of and access to specific classified NSI. The use of "Special Need-to-Know (SNTK)," "Must Know (MK)," "Controlled Need-to-Know (CNTK)" and other such designators is prohibited. They are not authorized for use as security markings.

Third, how are LIMDIS controls established and who may establish them?

Each DoD Component, including the Military Departments, determines which of its officials may establish LIMDIS controls for classified NSI under their cognizance. This is a matter deserving some reflection: If we want to avoid multiplying the number of confusing nicknames used for security protection, we must minimize the number of LIMDIS controls. Most certainly, the proliferation of LIMDIS controls will lessen their value. If many programs employ these need-to-know enhancements, then no one of them may be better off. If everything is special, nothing is special.

Remember, LIMDIS controls came into existence largely to replace bogus security markings such as SNTK, MK, and CNTK. The latter were often applied by program managers who felt that the standard security system could not protect their material, but they could not qualify for a SAP. Their abolition was precipitated by the General Accounting Office which held that the bogus markings often bore strong resemblance to SAPs. It is possible that we are undergoing transition pains, but security specialists can help ease the pain by understanding and explaining the rationale for LIMDIS controls to our clients.

In a similar manner, each DoD Component determines the procedures for establishing LIMDIS controls. They prescribe how to identify the information to be controlled and assign a nickname for the LIMDIS controls approved for information and data in the program, project, system, plan, or operation. In all cases, however, the degree of controls specified may not exceed those which are identified within the normal security system.

Summary

At this point it should be obvious that SAPs and LIMDIS controls are significantly different. Although they both emphasize the need-to-know principle, they adopt different kinds of formal security measures to restrict personnel access to, and distribution of, information that is classified in the interest of national security. Neither is approved without consideration of the additional costs and burdens imposed, because all security measures have a price.

The point is, however, that the need-to-know principle is the factor that regulates the flow of classified information, whether it is administered informally, formally as in LIMDIS controls, or through a special access program.

Figure 2 should help keep the two separate and distinct in our thinking about the need-to-know principle.

Clearly, then, LIMDIS controls need never be confused with SAPs. ■

Raymond P. Schmidt is Head, Information Security Policy, Department of the Navy.

THE THREAT TO WESTERN TECHNOLOGY

James W. Dearlove

Technology transfer means different things to different groups. To the manufacturer or to a research and development center, it represents an item or an idea to be sold at a profit. To an economic department of the government, it can represent a method of establishing trade and equalizing a balance of payments. To a political department, it may represent a method of establishing diplomatic ties and linkage. From the defense viewpoint, technology may well represent a national resource which should not be shared with potential adversaries for any reason.

In today's changing world, warmaking technology takes on an even more important role. It can multiply the international leverage of third world countries that would otherwise be of less concern to us. For example, the proliferation of chemical, nuclear, and missile technologies was highlighted during the recent Iraqi crisis, and those concerns continue even after that fighting ended.

Comparing the United States and Soviet space shuttles gives us a good starting point to understand the worldwide threat. Detailed study shows many differences between these shuttles, some subtle, others not so subtle. Differences such as the separate Soviet booster, which can launch other payloads, give the Soviets a visible probable advantage. On the other hand, internal computers and sophisticated electronics are the heart of the U.S. vehicle but are not easily seen.

We have been studying the Soviet program to acquire Western technology for many years and have learned more over time. In 1981, a KGB colonel, who was given the code name "Farewell" by the French, provided documents which allowed us to study, in detail, the Soviet program to acquire and use Western technology. I will discuss salient aspects of the Soviet technology acquisition program.

Since 1985, when Gorbachev began his rendezvous with destiny, the Western world has become closer to the Soviet Union. As part of that closeness, we have become more susceptible to the undesired Soviet acquisition of our technology. Today, with borders opening and political and economic barriers shrinking, a closer look at the Soviets reveals they have adapted their methods of acquiring Western technology to current circumstances.

In the early 1980's, we identified two major Soviet programs that support their efforts:

- The first is the trade diversion program for the acquisition of large amounts of dual-use equipment and related items for direct use in production lines. This is an export control issue and is being well addressed by individual national export control systems and the COCOM, or international control system.

- The second program is that of the VPK or Military Industrial Commission to target technical data, information, and one-of-a-kind items. This program is much more difficult to deal with and presents the greatest challenge to us today. The threat posed by this effort to acquire data, information, and technology transferred by person-to-person is where we need to place our greatest effort. It presents us with our greatest challenge.

The State Committee for Science and Technology (GKNT) acts as a collector and as the central processor for the national-level program. It also monitors the absorption and assimilation of Western technology by the defense industries. The GKNT knows very well the deficiencies of the Soviet Union and, with the assistance of a number of organizations subordinate to it, knows precisely where to go to obtain the desired information, technology, and equipment--the country, the company, and if necessary, the individual. GKNT negotiates scientific and technical contracts, bilateral ex-

State Committee for Science & Technology (GKNT)

Maintains priority listing of Soviet Deficiencies

Negotiates Scientific and Technical Contracts

Negotiates Bilateral Agreements and Exchanges

Works Closely with Academy of Sciences

Directs Information Gathering by Scientists, KGB, and GRU

changes and agreements with other countries as well as many individual companies.

The prestigious Academy of Sciences is responsible for conducting much of the basic research in the Soviet Union. It, too, however, is heavily involved in the effort to acquire Western technology. In fact, in the changing world of the Soviet Union, the Academy has even a greater responsibility to establish strong liaison with Western countries and add vigor to Soviet research. Because it is an "Academy of Sciences," it is able to open many doors to the world's academic communities, enabling it to serve as a very effective technology transfer mechanism. Note however, that recent controversies over control of republic academies and over increased pay and benefits for Academy scientists has been disruptive it its work.

Supporting both the Academy of Sciences and the GKNT are several organizations that make it possible for them to perform their functions so well. One is the All-Union Institute of Scientific and Technical Information (VINITI). VINITI has been described as the largest single producer of scientific and technical abstracts in the world. It selects information from 35,000 periodicals, containing more than one and one-half million articles from about 125 countries in more than 65 languages, which it then translates and distributes to its users. VINITI reportedly controls about 10,000 scientific and technical libraries and employs, on a full-time or part-time basis, more than 150,000 persons.

Finally, there are the Soviet KGB and GRU (Chief Intelligence Directorate of the Soviet General Staff) who play a major role in the legal and illegal acquisition of technology, information and equipment. The KGB Directorate "T" conducts operations to collect information and material on science and technology. The KGB also has numerous other directorates engaged in classical spy operations to obtain Western secrets or sensitive information. GRU officers, most of whom have a technical background and education, appear to concentrate more on the collection of information with direct and immediate military value. Recent information indicates an even more active role for the KGB in acquisition of sensitive but unclassified Western technical information.

British researcher Philip Hanson was given the opportunity to review some Soviet KGB documents acquired by the French in the famous "Farewell affair" of 1981-82 alluded to earlier. The French provided Mr. Hanson with only five of the thousands of documents documenting the Soviet technology acquisition program they received from "Farewell," and he wrote about them in his 1987 paper entitled "Soviet Industrial Espionage: Some New Information." From Mr. Hanson's work, as well as ours, we see that the Soviets have an extremely well orchestrated mechanism for determining their internal deficiencies, a means for determining what is available elsewhere in the world, and a very systematic method for promptly acquiring the technology, information, and equipment they need. The illustration, taken from his paper, reveals the kind of data the Soviets were interested in, where these data had reduced research time, and perhaps even where data corrected their efforts that would not have led to successful solutions. Most importantly, it became known that the Soviets were well organized and employed a responsive system to accomplish their technology transfer objectives.

Next, I will discuss some of the mechanisms for technology transfer.

There are as many technology transfer mechanism as there are ingenious minds. The illustration categorizes as legal or illegal some of these mechanisms, beginning with various open literature publications and progressing through the various

DATA FROM 1980 VPK REPORT ON ACQUISITION OF WESTERN TECHNOLOGY*

MINISTRY	Acquisition Tasks In Effect	Acquisition Tasks Completed	Material Acquired	Material Found Useful	R&D Projects Improved	R&D Projects Accelerated
			(samples/docs.)			
Aviation	369	98	255/4808	184/4027	353	143
Machine building	207	19	193/1580	175/1309	174	92
Radio	263	94	290/2475	266/1890	131	49
Shipbuilding	227	69	88/3456	86/2748	37	25**
Electronics	864	328	1443/4113	1478/2445	1796	635***
Chemical	209	38	790/1389	450/1208	55	175

**** SHIPBUILDING - 3 CUT OUT**
***** ELECTRONICS - 353 CUT OUT**

***SOURCE - 1987 REPORT - SOVIET INDUSTRIAL ESPIONAGE: SOME NEW INFORMATION LONDON: ROYAL INSTITUTE OF INTERNATIONAL AFFAIRS, HANSON, PHILLIP**

types of exchanges, business dealings, sales, and exploitation of captured equipment. Although there are numerous examples of technology transfer for all these mechanisms, my discussion will touch on only a few.

TRANSER MECHANISMS

LEGAL	ILLEGAL
Scientific Publications	Spying
Patents	Clandestine Acquisition
Databases	Coopting Personnel
Conferences	Dummy Corporations
Joint Ventures	Illegal Purchases
Sales Proposals	Diversions of Legal Sales
Trade Shows	Evasion of U.S. Controls
Business Visitors	Misrepresentations:
Students	• of level of technology • of end user • of foreign availability

Consider some of the problems we face with trade. Millions of tons of goods move daily in the world. The responsibility for assuring that these goods are being exported legally varies from country to country. Before the early 1980s a mere handful of people were responsible for the supervision of exports. Today, under COCOM and other efforts that help nations work together, the loss of sophisticated technology has been reduced, and from remarks recently made by Soviet president Gorbachev, they have been effective.

Today's world of international marketing and multinational corporations provides an environment that facilitates, in fact makes necessary, the operation of foreign owned companies in other countries. True ownership of these companies is often not known to the people or firms seeking to use them. This is an illustration of the problem that must be addressed by our respective export control organizations today. It also shows the extent that we in the intelligence service have to go to in order to get answers to the questions of today. Note that the source of this information is Carleton University of Ottawa, Canada.

SOVIET COMPANIES OPERATING IN THE WEST (1990)*

128 Soviet Companies Operating in Western Countries**

58 percent engage primarily in marketing of raw materials, products and technology

59 percent of Soviet companies located in Belgium, Finland, France, FRG, Italy and UK

718 million dollars invested in 128 companies.

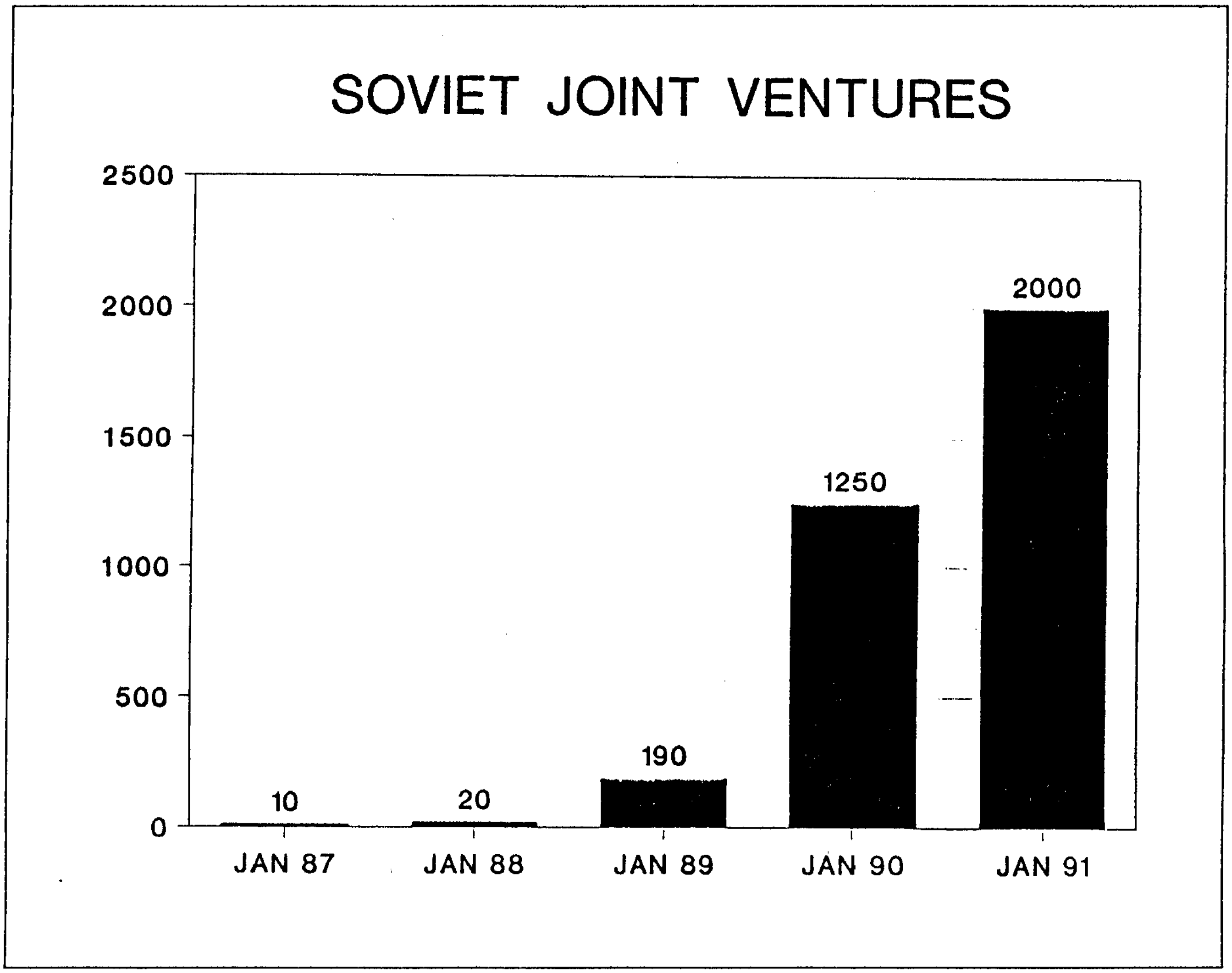
*Source: East-West Project, Carleton University, Ottawa, 1990
**Does not include offices of Intourist, Aeroflot or Chambers of Commerce

With the changing world comes changing ways of doing business. The joint venture is one Soviet response to the need for more technology and better business practices. This chart vividly illustrates the results of the lessening of tensions and the increased use of joint ventures in various stages of completion. The majority of joint ventures are not operational, and currently few are being concluded with foreign firms because of the declining Soviet economy and domestic instability.

Many of the joint ventures are not concerned with technical areas; rather, they deal with tourism and services such as hotels and restaurants. Those actual and proposed ventures involving technical areas, however, offer remarkable potential for technology transfer. The Soviets must have advanced technology to be successful in their military and industrial programs.

Here is a report of what one delegation of Soviets was able to do:

"A Soviet delegation of experts under the leadership of Alexander N. Gerashchenko, First Deputy Minister of the Aviation Industry, toured U.S. aerospace facilities. They were admitted to heretofore off-limits facilities and shown previously restricted hardware. Other meetings, unthinkable a few years ago, were also held with representatives of giant defense contractors. Whereas earlier Soviet visitors were greeted with chilly reserve and



distrust, the Soviets were now treated as potential partners."

The KGB, always ready to take advantage of an opportunity, has redefined its priorities so it will be able to work in the Western aerospace industry, to emphasize targeting of economic intelligence, and to make its services available to entities outside the communist party and government.

There are a large number of commercial, professional, technical, and government journals that publish a tremendous amount of information. They provide us with a wealth of data on the latest world-wide military and technological developments. Unfortunately, these same data quickly go to our potential adversaries.

The U.S. National Technical Information Service (NTIS) was established in order to make available to the American public the unclassified results of the research funded by our taxes. This repository is also open to anyone else in the world, including the Soviet Union, for a very small price. Many libraries and databases throughout Europe also subscribe to NTIS, thus indirectly making bibliographies and documents available to the Soviets. The Soviets can also access many such databases throughout the world by computer networking.

To illustrate Soviet access to Western databases, I would like to use, as only one example, the International Institute of Applied Systems Analysis (IIASA). An increasing number of electronic databases and networks are accessible in various, and often deceptively, indirect--yet legal--ways. The Soviets and East Europeans massively exploit the access of the Institute's computer network, as well as other Western European computer database network centers, to Western scientific and technical databases. Soviet and East Europeans have been able to access Western computer networks and major scientific and technical databases through the TYMNET, TELENET, and European space agency computer networks. For the past eight years, they have gained access to valuable data and documents. Through these networks the Soviets have been able to determine the contents of the database of the U.S. National Technical Information Service and, subsequently, to order documents.

A recently installed capability illustrates how technology facilitates the process of transferring information to the USSR. Previously, within the IIASA network, there were many inter-connections and the line capacities were limited. Today, the Soviets can bypass these problems using the Moscow Telenet--a satellite network that provides 1.5 megabytes of information from the same databases without the problem of having to utilize slow and complicated networks.

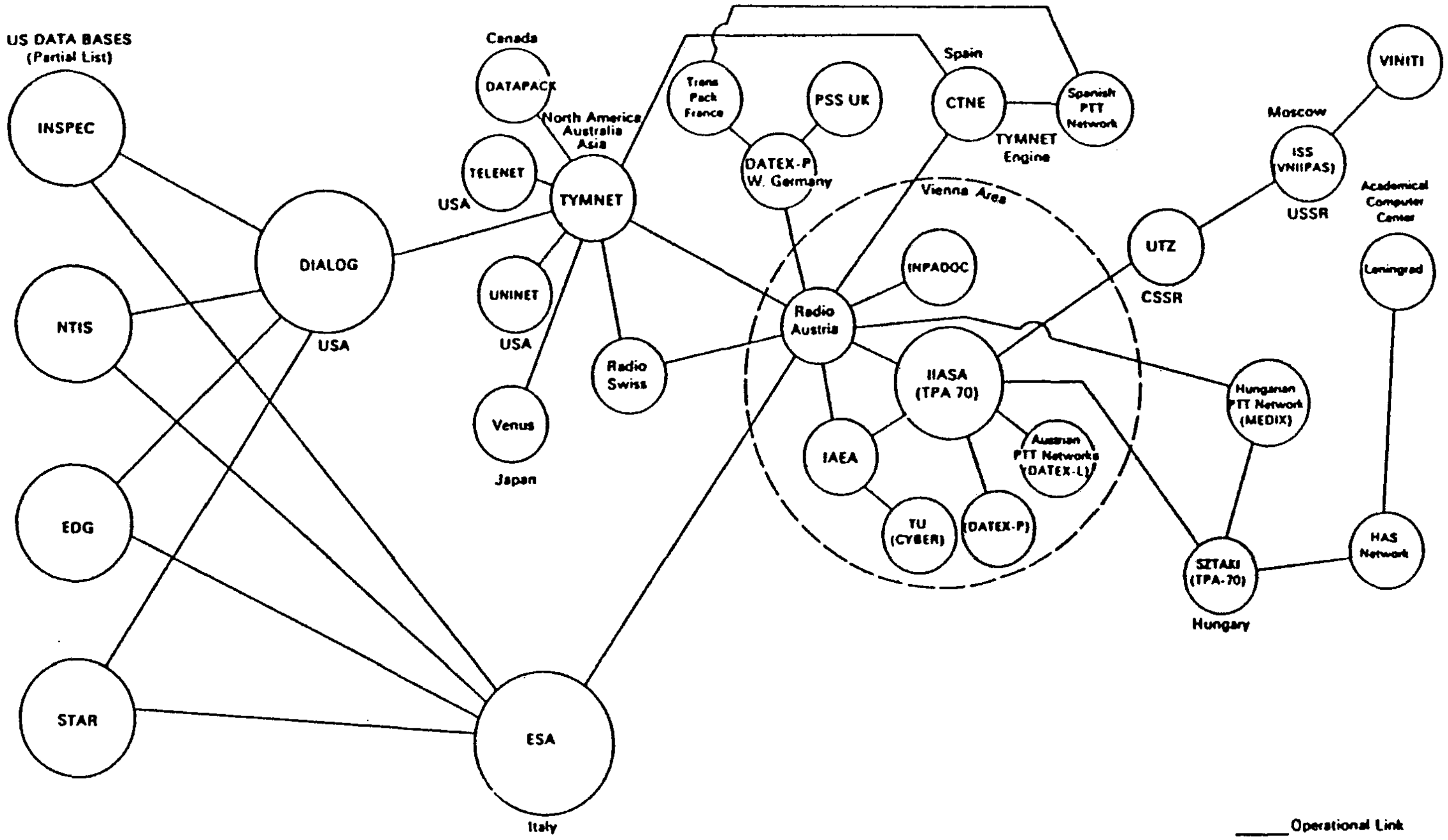
In an effort to inhibit this flow of technology, the U.S. Congress in 1983 gave the Secretary of Defense the authority to withhold certain types of unclassified, yet sensitive, technical data from public disclosure by restricting its dissemination. If necessary, additional control authority resides in the U.S. munitions list and the U.S. unilateral dual-use embargo list, referred to as the "Commodity Control List." Violations of these export laws are subject to criminal penalties.

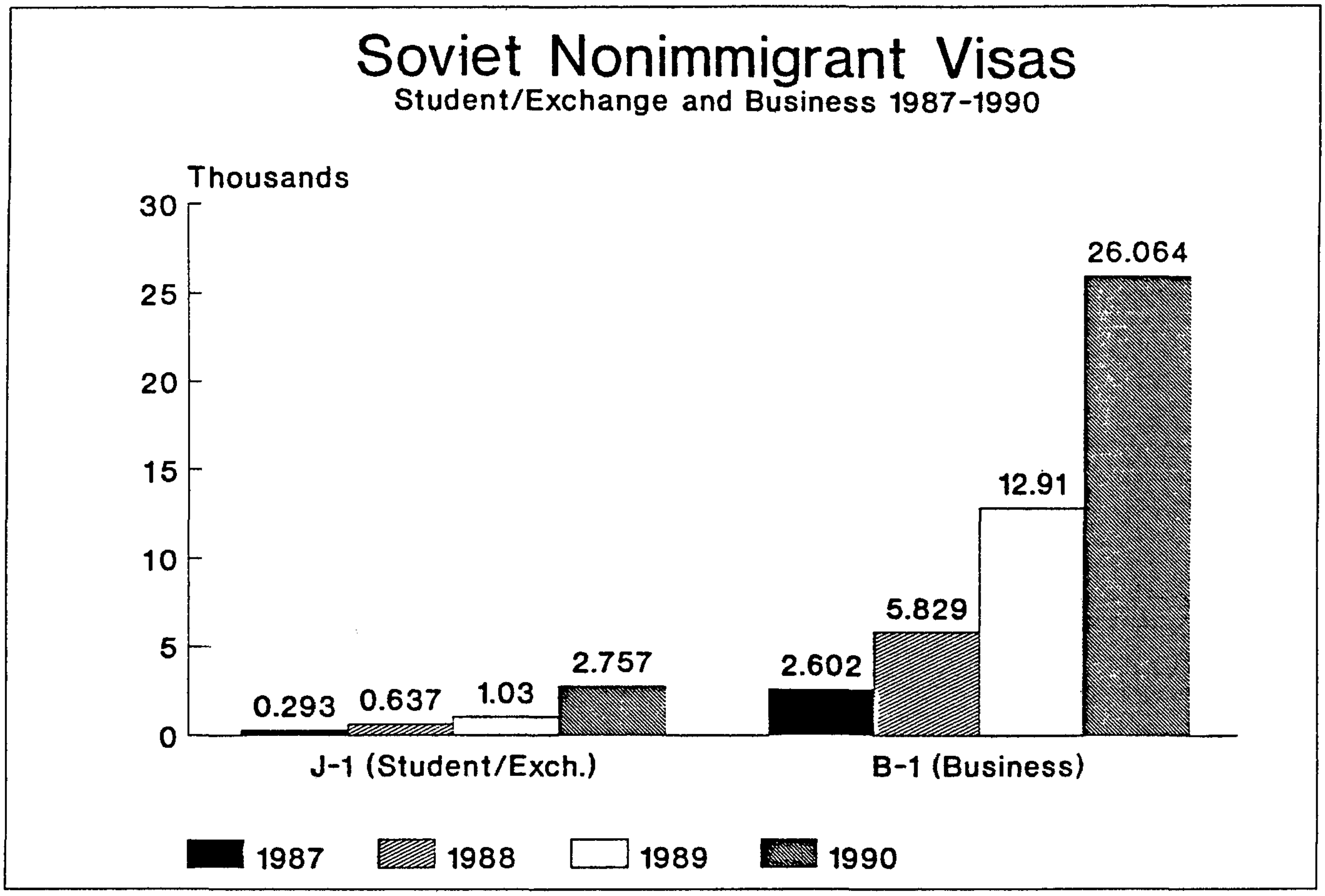
The Soviets have long recognized that one of the most effective technology transfer mechanisms is through person-to-person contact. One of the methods of achieving such contact, and sharing of scientific and technical information, is through the establishment of bilateral scientific and technical agreements with technologically advanced countries. To this end, the Soviets have established many such agreements with a large number of countries over the years. It was not until the 1970s that the first of 11 government-to-government bilateral agreements in areas of science and technology were negotiated between the USSR and the U.S. At the President's direction, three bilaterals of greatest concern were allowed to lapse in 1982. Today,

BILATERAL AGREEMENTS

Bilateral Agreements	Executive Agency	Active Projects/ Subprojects	Signed
Agriculture	DOA	3/19	1973/Ongoing
Atomic Energy	DOE	4/22	1973/1990
Energy-Non Nuclear	DOE	Undergoing Negotiation	1974/Cancelled 1982
Environmental Protection	EPA	12/37	1972/Ongoing
Health (2)	HHS	11/43	1972, 74/Ongoing
Housing	HUD	6/22	1974/Allowed to expire 1989
World Ocean	DOC/NOAA	3	1973/1990
Basic Scientifc Research	OSTP	24/47	1972/1989
Space	NASA	6/18	1972/1987
Transportation	DOT	4/15	1973/1988

WORLDWIDE COMPUTERIZED TECHNICAL INFORMATION NETWORK





two of the three, space and basic scientific research have been reestablished, and the energy bilateral is in the process of being reestablished. In the bilaterals of the 1970s, the flow of information and technology was predominantly in one direction -- towards the USSR. Today, we require all agreements to be studied closely to ensure that sensitive technologies are not compromised and that true reciprocity exits.

Next, I would like to review the change in the Soviet presence in the United States. While the number of non-immigrant visas issued to citizens of East European countries has remained relatively stable for the past four years, the number of visas for the Soviet Union increased ten times during the four-year period from 1987 through 1990. Business and student/exchanges grew from 2,895 in 1987 to 28,821 for 1990--a significant change when one considers things such as cost.

There was also a ten times increase in tourist visas during this period, from 5,500 in 1987 to 59,222 in 1990. Together with business and student visitors, the total of over 88,000 Soviets in the U.S. for 1990 serves to illustrate both the overall change in relations with the West, and the increase in potential for technology transfer through the person-to-person mechanism.

In summary, we have more Soviet visitors. Their reasons for coming are changing over the years. For example, many more tourists and business people are visiting. Some want to stay, and the Soviet government is very concerned about the loss of national creative power. I recently read that a Soviet citizen, a good research scientist who wanted out, was given additional security clearances so that he could not leave.

Finally, I would like to touch on several relatively new developments in the way the Soviets are conducting business;

First, defense conversion is in its third year, more or less. It certainly is not yet successful and some wonder if it is not really strengthening their defense industrial base instead of changing it to a civilian one.

GKNT - 18 NATIONAL S&T PROGRAMS

High-Energy Physics
High-Temperature Superconductivity
Mars
Human Genome
New Information Technologies
Technologies, Machines and Processes of the Future
New Materials
Advanced Biological Engineering Methods
High-Speed Ecologically Clean Transport
Ecologically Clean Power Engineering
Resource-Saving and Ecologically Clean Metallurgical and Chemical Processes
High-efficiency Food Production Processes
Combating Widespread Diseases
Construction in the Year 2000
Controlled Fusion and Plasma Processes
Safety of Population and National Economy Objects in View of the Risk of Natural and Technological Catastrophes
Prospective Telecommunication Facilities and Integrated Communication System
Global Changes of the Environment and the Climate

Second, the charge given the KGB chief Vladimir Kryuchkov by President Gorbachev to sweep the world for industrial and military secrets needed to transform the economy. We certainly have seen changes in the KGB organization and operation. It remains to be seen if they will be as successful as the Soviets expect.

GKNT Chairman N.P. Laverov provided this list of scientific and technical programs to the U.S. earlier this year. On it are their targets as well as some areas they are expert in. Most are dual use, having both military and civilian applications as in integrated communication systems for providing better inter-city and republic communciations. These systems also provide better military command and control.

The advantages gained from technology transfer allow the Soviet Union to improve its military capabilities. In many instances however, these same advantages may benefit the economy. They save billions of dollars for research, cut years off the research and development cycle, eliminate risks involved in any untested venture, and spur immediate countermeasures.

We have looked at some of the changes that today affect the Soviet technology acquisition effort and changes in the effort itself. The world is relaxing as the perceived threat diminishes. There are many new relationships that place the Soviets closer to sophisticated technology than ever before. Although they are designed to have a minimal effect on technology transfer, there are cooperation programs, such as those between our military and theirs, that would never have been considered before. For example, they are contacting Soviets who left the Soviet Union years before and now are working in our country. They are appealing to them to help the motherland with their technological ability. Along with all this, their real concern is that they are losing their real intellectual creative power.

SUMMARY

<u>**Soviet model still in effect**</u>

✓ Not as rigid
✓ Opportunity rich

<u>**KGB**</u>

✓ Demonstrating a flexibility to adapt to new events
✓ Possess new power to monitor joint ventures

The Soviets greatly depend on Western technology, more than any of us fully understood until the early 1980s. We have gained a better understanding of this dependence as our knowledge of their systems increases through more open access to their industry and their people. They are extremely persistent in their acquisition efforts. They will acquire technology at no cost if possible. They will buy it if necessary. They will even pay an excessive price for it if they must. If all else fails, they will acquire it clandestinely. The effort is centrally orchestrated at the highest level of the Soviet Government. They know their own deficiencies. They know very well, sometimes better than we, what technology and equipment is available from the free world, and they know exactly where to go to obtain it: the country, the company, the government installation, and if necessary--the individual concerned. In addition, they--especially the KGB--have shown a flexibility to adapt to events and to capitalize on them. We believe the problem of technology transfer to the Soviets is much more difficult today than in the past. We must all be aware and equally flexible in our response. ■

James W. Dearlove is Senior Intelligence Officer, Techology Transfer Branch, Office of Scientific and Technical Intelligence, Defense Intelligence Agency.