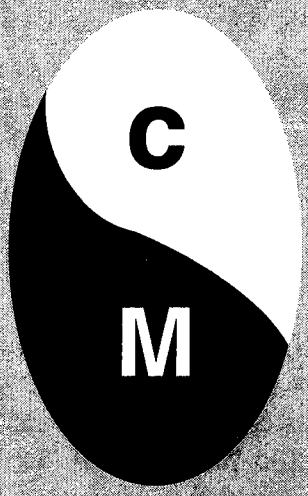


A PUBLICATION of the NATIONAL
CLASSIFICATION MANAGEMENT SOCIETY
VOLUME 1, 1996

Published by the National Classification Management Society. Mailing address: Executive Secretary, NCMS, 2017 Walnut Street, Philadelphia, Pennsylvania 19103. Editor of this volume: Raymond P. Schmidt. Editorial Review Board: Carol F. Donner, General Research Corporation; Marilyn H. Griffin, Naval Coastal Systems Center; James H. Mathena, Lockheed Martin Corporation; Arvin S. Quist, Lockheed Martin Corporation. Board of Directors Publications Oversight: Dr. Roger Denk, PERSEREC; Carol Donner, General Research Corporation. Publication Coordinator and Publisher: Sharon K. Carter, Executive Secretary. The information contained in this periodical and presented by the several authors does not necessarily represent the views of their organizations or the National Classification Management Society.

PURPOSE

The purposes of the National Classification Management Society are:

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

Members are encouraged to submit articles, think pieces, scholarly studies, and letters about any aspect of classification management and information security. As this issue is the last edition of *VIEWPOINTS*, all security subjects will be considered for inclusion in the *CM BULLETIN*, a bimonthly newsletter of the NCMS.

PERIODICAL OF THE NATIONAL CLASSIFICATION MANAGEMENT SOCIETY

TABLE OF CONTENTS

EDITORIAL COMMENTS

Do the people of the United States face greater or reduced threats to our security today than during decades of the Soviet Empire? Few issues are argued today with more passion. **Mr. Alan Thompson** argues for the affirmative--that the Cold War is over. In his personal conclusions, Mr. Thompson believes that this undeniable fact should lead us to less secrecy and faster declassification of official information.

Mr. Nicholas Eftimiades presents a contrasting view, if not an argument for the negative or a refutation of the underlying assumption that the world is now a safer place. As an analyst specializing in China, Mr. Eftimiades highlights important information about the most populous country in the world that received little public attention during the decades of the Cold War.

While neither Mr. Thompson nor Mr. Eftimiades intended to write point--counterpoint on this issue, their positions illustrate the role that *Viewpoints* was created to serve. We hope their articles help to inform debate and to encourage further study. Both authors, it should be noted, benefit from open discussion of the points they raise. Readers will draw their own lessons about the national security, the viability of threats, declassification, and the role of secrecy in our democracy.

In the feature article, **Mr. Charles Wilson** deals with the central concerns of the National Classification Management Society: those relating to classification management. He brings decades of experience and careful thought to what many professional security officials believe must be the focal point of reform--improving original classification decisions. Previous contributors to *Viewpoints* have presented useful analyses and recommendations on this point, but Mr. Wilson brings a singularly unique perspective as an official deeply involved with the many foreign governments with whom the United States has agreements to exchange or share classified information.

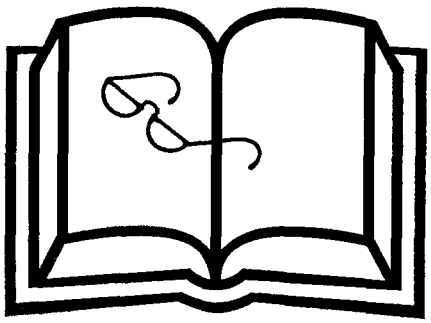
Mr. James Bagley serves the security manager whose responsibilities encompass dealing with foreign companies. As always, he offers specific advice to assist those who may not yet have become familiar with the complexities and interactions of entities involved in classified foreign agreements.

Mr. Calvin Wood explains his position advocating the universal adoption of risk management throughout the Executive Branch. Some security specialists are already expert in using this tool, but others may find his article helpful in understanding discussions swirling around the country. No one should miss his central thesis that risk management is an iterative process. It will be interesting to observe whether many organizations can afford to carry out a formal process, and what effect risk management employed in this manner has on the protection of classified information.

The final item included here is **Executive Order 12968.** It needs no further introduction, and undoubtedly will be explained and expanded many times in many ways.

This is the final edition of *Viewpoints*. Several years ago I had asked NCMS to find another editor and, in discussions with various officers, urged the exploration of alternative means of communications among members. This edition would have been published last fall if funds had not been required for other purposes. NCMS is evolving into a different professional society--preparing for the 21st century. I thank all the contributors, editorial review board, publishers, and readers for your support.

--Raymond P. Schmidt



REMARKS

by Edwin Alan Thompson

I want to quote a little bit of fiction to you by way of text for my "sermon." It is taken from the word by John LeCarre, his post-Cold War book, *The Secret Pilgrim*.

The book, by the way, was dedicated to Alec Guinness. I will not attempt to recreate his inflection. But I'll refrain from using my own words so far as I can refrain--and stick to the author's text.

The scene is a party attended by all the "old boys"--four generations of members of "The Circus." George Smiley is seated "on his throne of honour."

"It's over," George Smiley said...

"It's over ... Absolutely over. Time you rang down the curtain on yesterday's cold warrior. The new time needs new people. The worst thing you can do is imitate (yesterday's cold warrior)."...

"I only ever cared about the *man*.... I never gave a fig for the ideologies, unless they were mad or evil. I never saw institutions as being worthy of their parts, or policies as much other than excuses for not feeling. *Man*, not the mass, is what our calling is about.

"It was *man* who ended the Cold War in case you didn't notice. It wasn't weaponry, or technology, or armies or campaigns. It was just *man*. Not even Western man either, as it happens, but our sworn enemy in the East, who went into the streets, faced the bullets and the batons and said, we've had enough. It was their emperor, not ours, who had the nerve to mount the rostrum and declare he had no clothes.

"One day, history may tell us who really won. If a democratic Russia emerges--why then, Russia will have been the winner. And if the West chokes on its own materialism, then the West may still turn out to have been the loser. History keeps her secrets longer than most of us. But she has one secret that I will reveal to you tonight in the greatest confidence. Sometimes there are no winners at all. And sometimes nobody needs to lose.

"You ask me how we should think of Russia today....

"You ask, ...can we ever trust the Bear? You seem to be amused, yet a bit unseated, by the notion that we can talk to the Russians like human beings and find common cause with them in many fields. I will give you several answers at once.

"The first is no, we can never trust the Bear. For one reason, the Bear doesn't trust himself. The Bear is threatened and the Bear is frightened and the Bear is falling apart. The Bear is disgusted with his past, sick of his present and scared stiff of his future. He often was. The Bear is broke, lazy, volatile, incompetent, slippery, dangerously proud, dangerously armed, sometimes brilliant, often ignorant. Without his claws, he'd be just another chaotic member of the Third World. But he isn't without his claws, not by any means. And he can't pull his soldiers back from foreign parts overnight, for the good reason that he can't house them or feed them or employ them, and he doesn't trust them either. And since this Service (and this Society) is the hired keeper of our national mistrust, we'd be neglecting our duty if we relaxed for one second our watch on the Bear, or on any of his unruly cubs. That's the first answer.

"The second answer is yes, we can trust the Bear completely. The Bear has never been so trustworthy. The Bear is begging to be part of us, to submerge his problems in us, to have his own bank account with us, to shop in our High Street and be accepted as a dignified member of our forest as well as his--all the more so because his society and economy are in tatters, his natural resources are pillaged and his managers incompetent beyond belief. The Bear needs us so desperately that we may safely trust him to need us. The Bear longs to wind back his dreadful history and emerge from the dark of the last seventy or seven hundred years. We are his daylight.

"The problem is, we Westerners do not find it in us naturally to trust the Bear, whether he's a White Bear or a Red Bear, or both kinds of bear at once, which is what he is at the moment. The Bear may be in perdition without us, but there are lots of us who believe that's exactly where he belongs. Just as there were people in

1945 who argued that a defeated Germany should remain a rubble desert for the rest of human history....

"The bear of the future will be whatever we make of him, and the reasons for making something of him are several.

"The first is common decency. When you've helped a man escape from wrongful imprisonment, the least you can do is provide him with a bowl of soup and the means to take his place in a free world.

"The second is so obvious it makes me a little intemperate to have to mention it at all. Russia--even Russia alone, shorn of all her conquests and possessions--is a vast country with a vast population in a crucial part of the globe. Do we leave the Bear to rot? Encourage him to become resentful, backward, an over-armed nation outside our camp? Or make a partner of him in a world that's changing its shape everyday?...

"It's not only our minds we're going to have to reconstruct either. It's the over-mighty modern State we've built for ourselves as a bastion against something that isn't there any more. We've given up far too many freedoms in order to be free. Now we've got to take them back...

"So while you're out there striving loyally for the State, perhaps you'll do me a small favour and lean on its pillars from time to time. It's gotten a lot too big for its boots of late. It would be nice if you would cut it down to size...." [1]

At this point in the story, George Smiley leaves the party and leaves the Circus. This is part of his way of ensuring that new people with new thinking will be in charge.

He has reminded us that the rules of the game, indeed the rule of the world as we know it, have changed. Old enemies have yielded to glasnost and perestroika or whatever we call the present situation in Bear country.

The darkest corners and shadows are now in full light of day, and the future is unfathomable. And we are asked to reconsider our relationship to the Bear.

Like Eisenhower in his final Presidential address, George Smiley is also warning us of the dangers of the overweening power of the state and of special interests using and abusing the power of the state--all built up and based on a threat that is no longer there.

As you may have heard, much of my career has been devoted to digging out from under the avalanche of secrets. So let me conclude with a few personal observations based on that lifetime of digging.

A significant part of the power of the state which has too often been abused and flagrantly overused is the power of secrecy.

We are entering into a new world, as John LeCarre so eloquently reminds us, and the State's power of secrecy needs to be cut down to size--to fit its boots--to fit the new reality and a new two-sided vision of the Bear.

You all must help in making the proper fit. You can demand, you can build, you can insist that classification management properly and appropriately measures the risk and the cost of protecting secrets against the many advantages of openness. You can create programs which will encourage and strengthen challenges to classification decisions--aimed at stopping it if you can, limiting it if you cannot. And you can ensure that those who do challenge classification decision are honored and respected--or at least fully protected from reprisal.

Just do not let state secrecy continue to grow as though nothing has changed.

---

[1] John LeCarre, The Secret Pilgrim. c. 1990, Chapter 12.

Edwin Alan Thompson retired from the National Archives after serving 20 years as its first Director of the Records Declassification Division. He has served on the NCMS Board of Directors and as President in 1978-79. He was presented the 1995 Donald B. Woodbridge Award of Excellence at the NCMS annual conference in Orlando, Florida, on June 28th, 1995.

THE THREAT FROM CHINESE INTELLIGENCE OPERATIONS

by Nicholas Eftimiades

From the end of World War II until recently, the former Soviet Union and its allies were considered the primary military threat to the United States' global interests. As a result, intelligence services of the Warsaw Pact were given a great deal of attention by American intelligence agencies. Considerably less effort, however, has been dedicated to identifying and neutralizing the espionage activities of nations which demonstrated no comparable military threat. One such country is the People's Republic of China (PRC). Although it has the largest armed forces in the world, the PRC has never developed, nor is it likely to have in the near future, the military force projection capability to invade any nation outside Asia. Because the PRC does not pose a credible global military threat, the PRC's espionage activities go largely unchecked by US intelligence and law enforcement agencies, as well as America's policy making apparatus. The PRC does, however, aggressively conduct espionage against the US.[1]

The short-sighted allocation of America's intelligence resources makes the US woefully unprepared to protect its national assets from Beijing's espionage efforts. China's clandestine intelligence collection operations against military related technology have increased in number to the point where US agencies with counterintelligence responsibilities are overwhelmed by the sheer volume of cases. The PRC's intelligence operations against the US are at the level where senior law enforcement officials have publicly identified China as "the most active foreign power engaged in the illegal acquisition of American technology."[2]

Recent arrests made by the Federal Bureau of Investigation (FBI) indicate that the PRC is quite focused in trying to obtain data on US military technology. For example, in December 1993, Mr. Yenmen Kao was arrested in Charlotte, NC, for trying to steal classified defense items, including a Mk-48 torpedo (advanced capability), two F-404-400 engines (sales price $2 million) for F/A-18 (Hornet) aircraft, and an AN-APG-68 fire control system for the F-16 aircraft. The FBI arrested Mr. Kao after a six and one-half year investigation for conducting espionage and violating immigration statutes. Mr. Kao was identified as a PRC intelligence operative and has been deported to Hong Kong.[3]

This incident was not the first time China's intelligence services have attempted espionage to increase the People's Liberation Army's (PLA) force projection capabilities. In March 1993, Messrs. Bin Wu, Jing Ping Li, and Pinzhe (Peter) Zhang were convicted in Norfolk, Virginia, of illegally exporting advanced second generation night vision devices to the PRC via Hong Kong. Wu and Li established a company--Cimex International Inc.--to conduct the illegal transfers, which were accomplished by falsifying shipping labels. The devices were destined for use by the People's Liberation Army. When arrested by US Customs, Mr. Wu had approximately $400,000 in one of several bank accounts. Mr. Wu was identified as a recruited agent for the PRC's Ministry of State Security. In an odd twist, however, he was also acting as a double agent for the FBI. The US District Court (Eastern District of Virginia) found that Mr. Wu was betraying both sides and guilty of multiple export and related violations. He was sentenced to 10 years in prison.[4]

During the mid to late 1980s, PRC intelligence officers and recruited agents have been prosecuted or deported for stealing, or attempting to steal, classified manuals on the Mark-48 torpedo, blueprints for the F-14, aircraft carrier technology, Sidewinder missiles, technical data on Enhanced Radiation Device (neutron bomb) development from Lawrence Livermore National Laboratories, and National Security Agency documents.[5]

China's intelligence collection operations have increased in number to the point where US agencies with counterintelligence responsibilities are overwhelmed by the sheer volume of cases. It is only in recent years that the US Intelligence Community has begun to recognize the magnitude of the PRC's collection operations:

> If we are talking about violations of US law, the Chinese are surpassing the Russians. We know they are running operations here. We have seen cases where they have encouraged people to apply to the CIA, the FBI, Naval Investigative Service, and other Defense Agencies. They have also attempted to recruit people at our (nuclear) research facilities at Los Alamos and at Lawrence Livermore.[6]

Industrial espionage and illegal technology transfer are only one (very publicized) aspect of China's intelligence activities. And these collection

operations are likely to receive greater emphasis as future activities for China's foreign intelligence services targeting the US industrial and commercial sectors. High technology-related information, used to develop China's civilian and military industrial sectors, is of particular importance to Beijing.

Like other regional or global powers, the PRC leadership uses its intelligence capabilities to support its own military, political, and economic self-interest. And while Washington and Beijing enjoy a somewhat more than casual friendship, many of China's regional aspirations are not likely to be in America's interests. There are a number of longstanding territorial disputes in Asia, several of which involve the PRC. Contentious issues such as the ownership of the possibly oil-rich Spratly (claimed by six nations) and Paracel islands, and the independence of Taiwan show no signs of early resolution. In addition, the recent People's Liberation Army's naval build-up and the overall net increase of approximately 116 percent in military spending in the last four years is doing nothing to calm the fears of China's neighbors.[7]

China's build up of military forces, which relies in part on its intelligence activities, is designed to project forces to control contested areas. This build up has already spurred a naval arms race among a number of Asian nations. And while none of these events presents a direct challenge to the overwhelming power of US forces, questions of regional stability come into play. China's vast size, population, booming economy, and naval force projection capabilities give it a justified place as a regional power. Depending on Beijing's actions on contested land issues and its conduct of foreign policy, however, the PRC's military growth and development could eventually destabilize the Asia-Pacific region. Some of that military expansion can be directly attributed to Chinese intelligence operations in the US. Only time will tell whether Beijing's foreign policy apparatus is adroit enough to guide the region to stability and peace, and whether America's policy apparatus is adroit enough to recognize the significance of the events now occurring. Regardless, China's intelligence services will play an increasingly greater role in supporting PRC national policy objectives by targeting and exploiting the technological, economic, political, and military infrastructure of modern industrialized nations.

Nicholas Eftimiades is an analyst with the Defense Intelligence Agency and author of the book Chinese Intelligence Operations, (Naval Institute Press, Annapolis, MD., March 1994). *Portions of this article first appeared in "Closer Ties; More Spies," Proceedings (Naval Institute Press, Annapolis, MD., March 1994).*

Footnotes

1 Eftimiades, Nicholas, Chinese Intelligence Operations, (Naval Institute Press; Annapolis, MD, March 1994), pp. 1-3.

2 William Overend, "China Seen Using Close U.S. Ties for Espionage." Los Angeles Times, Nov. 20, 1988, part 1., p. 34.

3 Los Angeles Times, "FBI Arrests Chinese National in Spy Ring Investigation," December 05, 1993, part A., p. 4.

4 United States Court of Appeals for the Fourth Circuit, Record Nos. 93-5800(L), 5801, 5802. United States of America v. Bin Wu, Jing Ping Li, and Pinzhe Zhang.

5 Eftimiades, Nicholas, Op. Cit. For indepth analyses of these and other cases, see chapter 6, "Foreign Operations."

6 William Overend, Loc. Cit.

7 Xiao Bing and Qing Bo, "Can the Chinese Army Win the Next War?" (Chongqing, PRC: Jun 1993), in Joint Publications Research Service, JPRS-CAR-94-024-L, 5 May 1994, p.10.

A PROPOSAL FOR IMPROVING ORIGINAL CLASSIFICATION OF NATIONAL SECURITY INFORMATION

by Charles C. Wilson

Senior officials of Government and industry have devoted many hours discussing U.S. and allied classification and safeguarding programs, searching for a solution that can be applied to the handling of information produced by two dozen Federal agencies and thousands of contractors. Several major study efforts over the past five years indicate the scope and depth of their various intensive examinations of a subject that holds vital importance to every taxpayer, not to mention its critical role in shaping the future of this country:

-- The National Industrial Security Program Task Force was established by President George Bush in December 1990. It was comprised of representatives from both the Federal Government and industry. Their efforts led to the establishment of the first National Industrial Security Program (NISP) and an Operating Manual (NISPOM) for use throughout the United States. The goals of the NISP were to establish uniform national standards and reciprocity, to simplify security program administration, to reduce redundant security requirements, and to reduce costs.

-- The Presidential Decision Directive 29 Task Force was formed in April 1993 to update and streamline information security policy and to issue a revised executive order for classifying, safeguarding, and declassifying national security information. Executive Order (EO) 12958 was signed in April 1995 as a post-Cold War document directing the automatic declassification of 25-year old records by 2000 and establishing a complex new scheme for marking documents classified after the effective date of the Order. The essential national implementing directives are being written as this article goes to press, and virtually all of the changes effected by the Order have yet to be tested in practice.

-- The Joint Security Commission (JSC) was chartered by the Secretary of Defense and the Director of Central Intelligence in June 1993 to develop a new approach to security that would assure the "adequacy of protection within the contours of a security system that is simplified, more uniform, and more cost effective." The Commission made 76 recommendations, some of which were controversial, others that were innovative, some which were based on common sense, and still others previously agreed to by agencies cooperating under the existing policy structure. Obviously not everyone agrees with all 76 recommendations. For example, it has been argued that, to a great extent, the Commission looked at security concerns from an intelligence community perspective and therefore did not reflect the broader perspective of the entire Government. One of the most important JSC recommendations -- adopted in 1994 -- was to create a national Security Policy Board with oversight responsibilities and a reporting chain that leads to the Executive Office of the President.

-- Even Congress is getting involved in looking at security policy formulation. Senator Daniel Patrick Moynihan is chairman of a commission, created by the "Protection and Reduction of Government Secrecy Act," Public Law 103-236, which has reached the halfway point of its two-year examination of various matters.

"First, there is too much classified information at too high a level... and Second, safeguarding measures currently used are not directly related to the level of assigned classification."

Issues

The officials who have been involved in all such studies generally agree on at least two issues:

* First, there is too much classified information classified at too high a level -- some of it for long periods of time -- resulting in excessive costs for protecting files and storing classified permanent records in the National Archives; and

* Second, safeguarding measures currently used are not directly related to the level of assigned classification. In the future, they must be based on identifiable threats, careful risk assessments, and management of the risk to counter those threats.

For the most part, these officials agree that any solution to the problem of managing classified information and reducing attendant costs, as a first order of business, must tackle the process by which information is originally classified. The problems must be addressed at their source if we ever want to save resources over the years ahead.

In my view, we would not even be discussing most of these problems if we had a comprehensive program with uniform and consistent national standards -- and with training in their use -- for classifying information in the first place.

"[We need] a comprehensive program with uniform and consistent national standards--and with training in their use--for classifying information...."

The Process of Original Classification

It is the critical process of reaching decisions to classify information originally that I will discuss next. Many security and operations personnel have offered comments and helpful suggestions about the process or this discussion. Let me emphasize, however, that these are personal opinions based upon my experience and do not represent a coordinated Department of Defense or US Government position. Nevertheless, the subject is clearly in need of informed, rational discussion.

The basic problem that lies at the root of our troubles is the lack of a disciplined, uniform approach to reaching original classification decisions. In short, we need a national classification process. Without it, we can expect to face more intense pressure for security reforms to fix the problems that cause both a real and a perceived overabundance of classified and over - classified information. Such a decision-making process must begin with clear, uniform national standards. They should be suitable for all agencies and all agencies will have to use them. Fortunately, several agencies are taking action to demonstrate that such standards can be developed.

First, take a look at what the new and previous Orders say about the original classification process. Information cannot be considered for classification as "national security information" (NSI) unless it is owned or controlled by or for the Government of the United States.

Next, Executive Order 12958 states that "national security means the national defense or foreign relations of the United States." It defines "information" as "knowledge." Therefore, we must conclude that "national security information" is "knowledge that relates to the national defense or foreign relations of the United States."

Then, consider what the Order identifies as relating to the national defense and foreign relations. Information must fall under at least one of seven categories of information in order to be eligible for classification. These are:

1. military plans, weapon systems, or operations;
2. foreign government information;
3. intelligence activities (including special activities), intelligence sources or methods, or cryptology;
4. foreign relations or foreign activities of the United States, including confidential sources;
5. scientific, technological, or economic matters relating to the national security;
6. United States Government programs for safeguarding nuclear materials or facilities;
7. vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security.

Finally, we must look at who can complete this process. The decision to classify the national security information in one of these categories can be exercised only by a Government official who has been specifically designated as an original classification authority (OCA) under the Order. In other words, the OCA is acting for the President of the United States in making an original classification decision. It goes without saying, of course, that the OCA also exercises this authority derived from the President in determining what NSI should be declassified.

The OCA then decides what level of classification, and what corresponding degree of protection, to assign to the officially - owned or controlled NSI in order to preserve its value to the United States. It will be classified:

-- TOP SECRET, if unauthorized disclosure will cause exceptionally grave damage to the national security;

-- SECRET, if unauthorized disclosure will cause serious damage to the national security; or

-- CONFIDENTIAL, if unauthorized disclosure will cause damage to the national security.

Now, that appears to be simple and straightforward. You, and any other official with the professional and technical expertise, can become an original classification authority! But we know that this process has shortcomings, or at least that its application has fallen short of universal success throughout the two dozen or so agencies that exercise original classification authority. Remember, most officials agree that some information is incorrectly assigned a classification when it should not be, and that still other information is assigned an incorrect classification level, either too high or too low.

The proliferation of errors in classifying intelligence and diplomatic information creates confusion and brings the entire classification program into question. This fundamental problem has not been addressed by any of the studies to date, and must become a top priority for US officials.

Reservations About the Process

I admit that I do not fully understand the operation of the classification process described above, and I have been engaged in Department of Defense intelligence and security matters for about 35 years. Its implementation in our security programs seems to create confusion. For example, two categories of classified information that caused me significant aggravation over the years are intelligence information and the so-called diplomatic information -- reports generated at our foreign posts. Information carried classification markings that appeared in open sources, and, conversely, intelligence was released that should have been protected with a classification marking.

A significant part of our policy, planning, and weapon development efforts in the Department of Defense involves one or both these two categories of information. If documents are not correctly marked when originated, the error carries over to derivatively - marked documents and programs, multiplying and even legitimating the mistaken classification. It is precisely the proliferation of such errors and the failure of the NISP and PRD-29 task forces or the JSC to address such a fundamental problem that caused me to raise original classification as an issue. I believe that responsible officials in US information security programs must place this issue at top priority and begin to solve the problem now!

Suggestions to Improve the Original Classification Process

The fundamental goal of all information security executive orders and regulations is to classify and protect only that deserving of our limited time and resources, and to release the rest. There are probably several ways of approaching our task. I offer here several suggestions about how we can change the process so it becomes more effective and efficient in meeting that goal. They begin with refining key definitions, move into developing national classification standards, and as a final step require linking classification levels with safeguarding and accounting measures.

Definitions

Security officials are generally highly skilled in using words, so I will caution that this is more than a question of semantics. We should develop a better sense of what we mean by "national security information," a long-standing term of art. NSI encompasses more than information that directly relates only to the national defense and foreign relations of the United States. For example, economic and emergency preparedness matters are already listed in EO 12958, but they cannot be confined to the national defense and foreign relations arenas; clearly, they must be included in the definition as well. And NSI involves knowledge relating to national activities as a whole, rather than strictly to national security programs. Finally, those officials designated as OCAs know that the information they classify should pass a judgment test that makes the NSI of special importance. Therefore, our new definition of "national security information" becomes "knowledge that is of critical importance or value to the nation." I would stop right there. Obviously, we can explain and illustrate, but nothing else needs to be added to this basic definition.

We should also sharpen our definitions of the three classification levels. Here are examples of how they might read:

* TOP SECRET shall be assigned if loss or compromise of the information could cause extremely grave damage to the nation; that is, it would result in actual -- or near--irreparable harm to a specified national interest (e.g., plan, program, project, system, operation, human life, economic endeavor) which I will discuss later.

* SECRET shall be used if loss or compromise of the information could cause serious damage to the nation; that is, it would result in harm that could not be easily rectified.

* CONFIDENTIAL shall be used if loss or compromise of the information could cause damage to the nation; that is, it could result in harm that could be rectified, but with some lesser degree of time, effort, money, or other resources than for SECRET.

A third area of definitions needing clarification, which I have already mentioned, deals with the several categories of NSI that can be considered for classification. The current definition includes "national defense" and "foreign relations" of the United States. If one closely analyzes the categories, however, terms appear that might fall outside these two areas. For example, we note reference to scientific and technological matters, economic

matters, and foreign activities in addition to foreign relations and national emergency preparedness plans. These appear to be major subsets of NSI of equal importance to the nation as foreign relations or defense information. Law enforcement and other kinds of information that are often classified are not even mentioned. So these basic definitions deserve our attention, and each agency or department of the Government should better identify the broad categories of information they generate that are of critical value to the nation. This may take time, but OCAs should be able readily to identify what information they classify.

"We need greater consistency in deciding what information in the [authorized] categories deserves to be classified....[An] agency or agencies [would] have primary jurisdiction over each category....[The proponent agency would explain and user agencies] would learn the rationale for classification and this [policy agreement] process itself should help bring about more consistent classification decisions....The major product would be useful master classification (and declassification) guides."

National Classification Standards

National Classification standards would help because we need greater consistency in deciding what information in the categories deserves to be classified. One way to accomplish this would be to determine which agency or agencies have primary jurisdiction over each category, to have them identify sub-categories of more specific information, and to rank these in order of importance or value to the nation. This will lead directly to assigning a classification level for each. Understandably, such an undertaking would require the best minds and most experienced original classifiers, but the consequent clarification and consistency would prove to be invaluable.

Here is how such a development process might work. The Department of Defense would take the lead on defense plans; the Department of State would take the lead on foreign relations; and the Central Intelligence Agency would take the lead on national foreign intelligence matters. They would develop lists that would be reviewed and coordinated until satisfactory resolution of inconsistencies was reached; we should expect legitimate differences of opinion and use our best efforts to distinguish among the divergent viewpoints. Each agency that generates, works extensively with, or uses the sub-categories would have an opportunity to participate in the process. Agencies would learn the rationale for classification and the process itself should help bring about more consistent classification decisions. A mechanism for resolving disputes must recognize concerns of both the agency of primary jurisdiction and others.

The major product would be useful master classification (and declassification) guides. Several highly centralized agencies already have such guides. Each agency that develops specific guides for programs and projects would have access to the master guides and supplement them to fit particular needs. If the guides were automated and agencies linked by secure nets, we might facilitate updates and cross-referencing of similar and related subjects. Thus, an OCA at Defense or State who is dealing with foreign relations information would have fingertip access to the same guidance for making a new original decision.

"Classification guidelines are related to the accounting and safeguarding requirements for each level of classification."

Linking Classification Levels with Safeguarding and Accounting Measures

I have developed a strawman chart (Figure 1) showing suggested baseline accounting and safeguarding measures as they might be applied to the three levels of classified information. It is notional rather than prescriptive, but it closely approximates what both experience and judgment suggest is workable, based upon the value of the information.

OCAs should be made aware that classification guidelines are related to the accounting and safeguarding requirements for each level of classification. Surprisingly, this reasonable expectation meets with resistance among some people; the JSC report even urged that the two areas need not be coupled in certain cases. But the JSC also noted that radical changes are needed in the way the classification process operates to restore its credibility. What better way than to ensure uniformity and consistency by training OCAs in a rational set of workable rules!

Designation	Decision*	Transmission**						Reproduction**				
		Reg Mail	Hand carry	Mil/Dip Courier	Comm-ercial Encryption	Govt. Encry-ption	Permission of Origin	Permission of Supv.	Cy No.	Serial No	Desig. Equip.	Witness
Top Secret	Loss would cause exceptionally grave damage to the nation. For example: reveal information that would result in a major diplomatic debacle, compromise the details of strategic war plans, reveal a critical clandestine source, reveal the development and application of a state-of-the-art technologicall innovation that gives the U.S. a singularly unique warfighting capability developed at great expense, etc. Only the most critical information would fall in this category.			X		X	X		X	X	X	X
Secret	Loss would cause serious damage to the nation. For example, the untimely revelation of the information could result in the impairment of a diplomatic initiative, reveal the results of intelligence analysis without revealing source; reveal the plans for the conduct of military operations, reveal vulnerability of fielded weapon systems, etc.	X	X	X		X		X			X	
Confidential	Loss would cause damage to the nation. (The term is too vague). For example, reveal the operational capability of fielded systems or existence of new developmental efforts, reveal the existence of intelligence analyses that could be supported by open sources, etc.	X	X	X		X					X	

FIGURE 1

Designation	Decision*	Recordkeeping**							
		Disclosure Record	Distr/.	Receipt/ Dispatch Records	Internal Distribution Records	Serial No.	Cy No.	Change of Custodian Inventory	Destruction Certificates
Top Secret	Loss would cause exceptionally grave damage to the nation. For example: reveal information that would result in a major diplomatic debacle, compromise the details of strategic war plans, reveal a critical clandestine source, reveal the development and application of a state-of-the-art technologicall innovation that gives the U.S. a singularly unique warfighting capability developed at great expense, etc. Only the most critical information would fall in this category.	X	X	X	X	X	X	X	X
Secret	Loss would cause serious damage to the nation. For example, the untimely revelation of the information could result in the impairment of a diplomatic initiative, reveal the results of intelligence analysis without revealing source; reveal the plans for the conduct of military operations, reveal vulnerability of fielded weapon systems, etc.		X	X					X
Confidential	Loss would cause damage to the nation. (The term is too vague). For example, reveal the operational capability of fielded systems or existence of new developmental efforts, reveal the existence of intelligence analyses that could be supported by open sources, etc.		X						

FIGURE 1

* The decision to apply one of the classification designations would be based on the value of the information in terms of damage to the nation in the event of compromise. Implicit in the decision (based) on the value and likely damage) is that a given set of mandatory safeguarding standards shall apply. One or more of the use, or storage (i.e., the environment) eliminate the risk which the standard is designed to counter (e.g., production and use in a RESTRICTED AREA may negotiate against the need for internal receipts). The result of the decision to place information in a classification category otherwise would result in the mandatory standards. The decision also must take into consideration the facts that no single security procedure is adequate to protect against loss, theft or espionage, and that it is not realistic to attempt to achieve absolute protection. Security-in-depth has been and must continue to be a guiding principle, applying risk analysis to the environment in which the information is generated, transmitted, and used.

** Listed safeguards and accounting are representative only.

Make Better Use of Freedom of Information Act (FOIA) Exemptions

All officials who create or originate information can make better use of the FOIA exemptions to withhold from public release certain information that has, up to this time, been classified simply to protect it from such disclosure. Of course, standard procedures and markings among agencies would be required, as well as training of originators and tighter control over the original classification process.

"If an OCA cannot justify the costs or is unwilling to abide by the accounting and safeguarding strictures, perhaps the decision to classify needs to be reevaluated or the information should be classified at a lower level."

Basis for Expecting Improvements in the Process

This proposal rests on faith that operations and security specialists can reach professional agreement on issues that involve potentially significant cost savings, that can result in better protection of classified national security information, and that deserve to be understood not only by practitioners in Government and industry but by taxpayers and citizens as well. I suggest four conditions for adoption of the linkage proposal:

-- We can reach agreement on the categories and sub-categories of information that may be classified at the three levels, based on their importance and value to the nation;

-- We develop more precise and consistent definitions of TOP SECRET, SECRET, and CONFIDENTIAL;

--We seriously enforce classification rules as required by EO 12958; and

-- Agencies accept comprehensive baseline accounting and safeguarding standards for the three classification levels based on the agreed definitions and guides.

With such standards and processes in place, automation among OCAs would bring about savings not currently possible. OCAs would have available on-line not only the most current guidance for determining classification at each level, but also the cost consequences of classifying information at a given level (based on the linked accounting and safeguarding requirements). If an OCA cannot justify the costs or is unwilling to abide by the accounting and safeguarding strictures, perhaps the decision to classify needs to be reevaluated or the information should be classified at a lower level. This proposal is not blind, however, because accounting and safeguarding requirements could be replaced by prescribed compensatory measures that still achieve the requisite security protection. The important point to note here is that the OCA would be making an informed decision about such matters at the time of original classification. A badly needed discipline would be introduced into the process.

I believe that the above proposals, if aggressively pursued, can lead to a much more viable information classification regime and thus reduce costs related to the entire realm of activities related to the protection of information. I am concerned that, if this is not done, those who currently espouse eliminating all controls and accounting requirements for Top Secret information, for example, will whittle away even further on safeguarding measures. This steady erosion of protection for collateral classified information would vastly increase the prospects for its compromise, and leave military personnel dangerously exposed in future conflicts. Our country cannot afford to wrap all classified information in cocoon-like special access programs. Nor can we afford to lose our heavy investments in technology and highly-skilled personnel through the inconsistent application of loose safeguarding measures adopted at the discretion of countless officials. This "chain" is certainly no stronger than its "weakest link."

In closing, I want to lend further credibility to this proposed process by addressing its application to automated technology. Information in paper and microform environments is generated, identified, processed, transmitted, stored, accounted for, and destroyed; these functions are also performed by an automated information system (AIS). A study by automation information experts has demonstrated that the means are available to replicate most if not all accounting and control functions using new technology in an AIS. In time, other protocols will be developed that may realize the objective of using technology to solve problems that other technology has created. We ought not throw up our hands and deny ourselves better approaches to classification management just because no one has found an answer yet, or worse, that "it was not invented here."

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

The Impact of Globalization on a Cleared Company: The Role of a Security Manager

by James J. Bagley

Background

This is the first of several articles I intend to write on this and related subjects. Obviously, the articles will address the subjects in broad generic terms and will not cover all of the related issues.

In an earlier outline, widely distributed throughout the National Classification Management Society for comment (principally favorable), I introduced many topics and set down my views on what the responsibilities of a Security Manager (SM) would be in a "globalized" world. I pointed out how previously disassociated programs often handled by a variety of personnel in both industry and government interacted. Furthermore, I noted how those various programs, when combined, represent the totality of information security issues which affect how both Government and industry will operate in a far broader and interactive world.

It is interesting to note that information security problems in the Government closely match those in industry, with one important difference: It is the Government which sets the tone, issues the regulations, and is responsible for compliance within industry. In a sense, the Government is in worse condition than industry because fewer people are available to be responsible for a greater number of programs and their contracts. As a result of "downsizing," many of the older and more experienced personnel have left and less experienced personnel are in charge. And it should always be remembered that a classifier is responsible for his or her classification actions until the information is declassified and all distribution limitations have been removed.

These indeed are "parlous" times, and this condition will remain for years to come. That is, it will prevail until the people now in charge attain, through trial and error and experience, the ability to decide what is important and requires protection and have the will to manage it.

Intent

First, I will take a new and broader look at the role of an SM in the identification of technology and information developed under Government auspices. Alternatively they may be developed under private auspices for Government application so that a company can take the steps to transform such information or technology into products or services which can be offered for sale or distribution to a broad international market.

Second, I would like to make the SM aware of the complexities and interactions involved when a company enters into an agreement or a joint venture with a foreign company for research and development, into a multinational contract, into a joint product or manufacturing development, or into a joint marketing arrangement. The SM should also be prepared to handle situations wherein a cleared US company is acquired by a foreign corporation/ company (in whole or in part), or makes an acquisition of a foreign corporation or company which is engaged in defense business in its own country or does business in the US as a Government (sub)contractor and which must have access to US classified or controlled unclassified information.

Each of the situations present to a SM individual problems, problems in which he or she may not play a major role, but problems which the SM must be aware of and have a feel for the complexities of the issues involved. Obviously, if there is the possibility of a foreign national or representative of foreign interest (regardless of citizenship) requiring access to classified information, export controlled information, or that unclassified information which has been designated as sensitive by a company or the Government, the appropriate Government laws and/or regulations apply.[1]

At the same time however, there are other less obvious implications and involvements in which an SM can play a role: the development of or ownership or access to patents and trademark information, copyright information, proprietary and privacy information, information which may not be released to the public without proper authority.[2]

To further aggravate the complexities of globalization on an SM there are foreign corporate governance and oversight, foreign finance, the role of banks in oversight and management of companies which are indebted to a bank. There have been many studies[3] on how foreign companies are governed and how foreign bank personnel may, and do, serve as directors of companies to which a bank has made business loans. Such practices are alien to US banking practices. In fact, it can be illegal for an officer of a loaning bank to serve on such a board.

There are many instances where foreign banks play an active role in the management of a company to which it has made loans and may insist on having access to any information which relates to the company's operations and management. In the US directors are expected to be independent of management. At the same time, US directors are expected have a significant oversight role of the total workings of a company including membership on committees required by the By-Laws.

Under the FOCI provisions of the *Industrial Security Manual*, and now the *National Industrial Security Program Operating Manual*, US directors serve on a company's Government Security Committee (GSC) as well as other required committees. An SM serves as the principal advisor to the GSC and attends its meetings. The chairman of the GSC must concur in the appointment of a Facility Security Officer nominated by management. The SM is also responsible for the preparation and oversight of a Technology Control Plan when required by the NISPOM and the ITAR.

There is another situation where an SM can be involved--compliance with the Foreign Corrupt Practices Act. A recent article in the *National Law Journal* citing recent cases makes an important point:

> "The perception among US companies generally is that only foreign agents and workers demand bribes. The history of cases, however, indicates otherwise. Americans are not only active in, but often initiate, offshore wrongdoing.
>
> "Consequently, employee screening should be a priority for companies before assigning offshore personnel, particularly management or executive positions. Corporations also should conduct thorough background checks on key members of joint ventures or other business partners. Many corporations do not perform these basic procedures, or do so perfunctorily."[4]

Under normal circumstances, it is the SM, acting alone or in concert with the company counsel, who takes a leading role in developing special briefings as part of the company's overall security briefing programs. When an event occurs, the SM either undertakes an investigation or supervises those personnel who may make an investigation. And, finally, the SM will be part of the company review and investigative process.

What Should an SM Know?

As the scope of an SM's responsibilities grows, it is mandatory that an SM have at least a working knowledge or understanding of all facets of a company's "globalization" program, especially that part of the program which involves the generation of information which a company considers to warrant protection for itself, the Government, or both. An SM is in a unique position, whether in Government or industry, to have a broad overview of a company's business or the mission of a Government agency.

Because of recent emphasis on the development of "threat models" the SM should have access to and be aware of any threat which could jeopardize the integrity of information generated by or in the possession of the organization.

The SM should also have direct knowledge or oversight of export control matters, including the laws and regulations of the participating foreign partners.

The SM must know how to protect a company from non-compliance with national security and foreign policy requirements.

Similarly, the SM must participate in the development of international program agreements, especially those which will involve the transfer of personnel between a US and a foreign partner wherein each individual involved in the agreement will have access to or possession of information under restrictive controls of the other; and the SM should assist in establishing protective standards for information that is developed jointly by the participating partners.

It is essential for the SM to have knowledge of security (personnel, physical and information, including computer security) practices of each of the foreign governments involved in a partnership agreement, and to be aware of the Government-to-Government agreements in effect which could affect an agreement, especially access to classified and proprietary information.

The SM must have knowledge of US and foreign disclosure policies and procedures, international patent exchange agreements, joint or multinational R&D agreements wherein contractors are involved, and treaty obligations, such as the Nuclear NonProliferation Pact, international armaments collaboration, agreements with NATO and non-Nato countries, relations with Pacific Rim countries, and Chemical and Biological Proliferation requirements.

In another area, the SM needs competence in US and foreign government controls on the dissemination of unclassified sensitive information and that foreign information designated as Restricted, which may be imposed by contract provisions or foreign laws and regulations.

Of course, the SM is required to understand US export control regulations and the same regulations of a foreign partner.

We cannot overlook the need for a solid grasp of Defense, State and Treasury Department Regulations governing foreign ownership, control, and influence and the regulations of the foreign partners, as well as manufacturing and R&D agreements and acquisitions, mergers, takeovers, joint ventures and the international financing of defense companies.

Interpersonal Relations

Globalization generally means the placing of foreign personnel in a US company, and US personnel in a foreign company in accordance with a partnership agreement. What are some of the most common problems?

First, an assumption that has proven to be accurate over time. In general, foreign personnel are more security conscious than US personnel; have a better knowledge of how far they can go in revealing their corporate or government "secrets," probably having signed an Official Secrets statement with their government (the consequences of unauthorized disclosure can be severe); know what can be revealed, or must be withheld; and usually are well briefed.

On the other hand, and as a general observation, Americans talk too much and are too ready to boast about what they know. As a consequence, Americans frequently disclose, deliberately or through carelessness, the "family jewels." Usually, Americans are not well briefed. And, all too frequently, top management is not briefed, and, all too frequently, they are the leakers.

What to do? Brief, brief, brief. There should be information control programs in place which should be drafted when a partnership agreement is being considered, covering the categories of information which should be controlled as internal matters, the types of information which would normally require pre-approval of the EAA or the ITAR and possibly the contracting activity, and the types of information for which security clearances would be necessary for foreign personnel. Remember that pre-approval of certain agreements is required by the ITAR and that contracting activity approval is also required.

Remember that, even when a foreign person is cleared for access to classified program information, an export license is required. See ITAR and relevant contract.

SMs should remember that their closest ally should be the company counsel, but some inexperienced counsels may not be sophisticated in security matters. It is the SM's job to educate the counsel. Remember also that, when a company under FOCI has a GSC, that committee is also responsible for export control oversight.

Where Is The Office?!

It is increasingly popular for US companies to have policies which permit full-time employees who split their work time between home and office and who communicate with their offices, and possibly their office computer, by means of a communications modem.

Being interested in this new phenomena and its possible effects on information security programs, I made an informal survey of a dozen or more companies throughout the country to ask whether the companies had policies in place to cover situations which could involve the employee doing company work at home. I was particularly interested in those employees who had R&D work assignments involving projects which might lead to the development of technology, concepts or ideas which the company could consider to be proprietary, or which, over time, might become classified if the information was being done under Government auspices regardless of whether the funding source was the company, Government, or a combination of both. I also surveyed several government activities to get a feel for their procedures. The results, for both industry and government:

- Very few organizations had workable and enforceable employer-employee agreements in place which spelled out the rights of the organization or the employee to information developed by an employee working off-site. Or, of greater importance, there were few rules covering an employee's access to his or her work computer from home or off-site. (This was a particular problem when an employee was working at home on ideas for new products which might be patentable or ideas which might be proprietary.)

- In those few instances where there was an agreement, the agreements appeared to be deficient as to who was covered, such as non-technical employees who would normally have access to the information, but would not be participants in its development. For example,

agreements overlooked finance, personnel, management, contracting personnel, and consultants. At times, sales, marketing, and publicity personnel were not covered, and contracts with outside publicity firms did not contain enforceable limitations on unauthorized disclosure.

■ There is a need for recognition of the impact of globalization problems in employer-employee agreements as well as any agreement, regardless of form or structure, which involves the creation of information which is either proprietary to a company or which involves government information classified or designated as requiring protection from unauthorized disclosure.

Agreements with foreign companies should include enforceable employer-employee agreements and cover, when appropriate, country practices, and the general differences between US and foreign practices. All personnel should be covered, with exceptions to be made only by senior management personnel. No exceptions should be allowed for rank or position in the organization.

Conditions by which an employee, authorized to work at home or off-site, may have access to information which is subject to protection as classified or proprietary must be clearly stated. I think that everyone will agree this is a pretty full plate. However, it is realistic in the light of how SMs of both Government and industry will have to work in a globalized world. And in spite of our personal thoughts, globalization is with us and will stay.

Yes, there will be "good guys" and "bad guys" and, at times one will replace the other, depending on issues and circumstances. However, that possibility only makes the need greater for knowledge of the issues and oversight of the possibilities. Although it appears that in the DoD, for instance, there will be a greater regulatory reliance on Government intelligence sources for information on foreign activities, there is an old salesman's tale that is particularly relevant. "Always know your customers, their products, sales philosophy and how they operate." No intelligence source can provide that information, and it is that information that can make or break a company. Intelligence can provide a broad brush awareness, overall political information, and some background. Such information is only one piece of the puzzle, however. Don't "bet the farm" on only a piece of the information.

James J. Bagley is one of the NCMS founders. He retired from Navy service after many years in a succession of responsible senior positions, and is now President of R.B. Associates in Falls Church, Virginia.

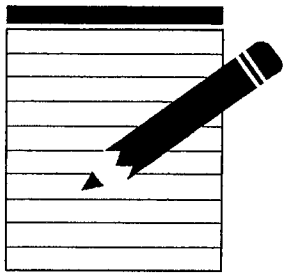
References

(1) ITAR, EAA, Section 721, Defense Production Act of 1950, as amended by Section 5021, Omnibus Trade and Competitiveness Act of 1988, (PL 100-418). See also Section 2-304, NISPOM January 1995.

(2) Title 35, USC, Patents and Trademarks; Registrar of Copyrights, Library of Congress; Freedom of Information Act, 5 USC 552; "Understanding Controls on Unclassified Government Information," *Viewpoints*, NCMS, Vol. 1, 1993.

(3) "Boards, Directors and Foreign Governance, Trends in G7 Countries Over the Next Ten Years," Oxford Analytica LTD, September 1992.

(4) "Complying With The Foreign Corrupt Practices Act," *The National Law Journal*, April 17, 1995.



IMPLEMENTING THE RISK MANAGEMENT PARADIGM

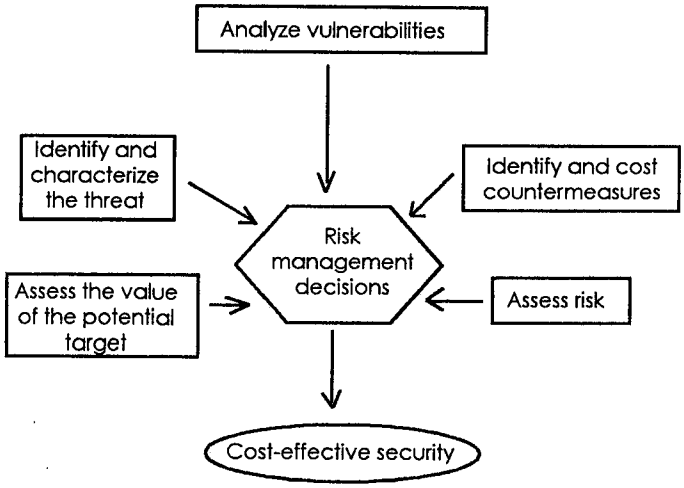
Calvin A. Wood

This paper addresses the most important ***concept*** expressed in the Joint Security Commission interim report, ***Redefining Security***. That concept is that ***we can and must provide a rational, cost-effective, and enduring framework using risk management as the underlying basis for security decision making***. In the process, I will discuss the origin of the risk management model proposed by the Joint Security Commission, relate it to the model used in the National Operations Security (OPSEC) Program, and discuss some issues which will need to be resolved as we move to implement this new (actually old) risk management paradigm to redefine security.

Incidentally, I am not promoting the National Operations Security Program. However, I have heard such comments as OPSEC is the same as risk management -- that it ***is*** risk management -- and that it is an administrative function versus an operations function versus a security function. I put these comments into a category with the phrase "All dogs are animals, but not all animals are dogs." Operations security is but one application of risk management. There are many ways in which risk management can be applied, and it should be applied differently according to the environment in which it is being used. What we need to strive for is a model, versus a specific tool, which can be applied equally well regardless of the environment in which it is being used.

Joint Security Commission Report

The Joint Security Commission was convened on June 11, 1993, to develop a new approach to security that would "assure the adequacy of protection within the contours of a security system that is simplified, more uniform, and more cost-effective."[1] This new approach, addressed in various places and ways within the commission's report, *Redefining Security*, is made clear in Chapter 1 by the caption "**Implementing the New Paradigm--Risk Management.**" The report states that we "can and must provide a rational, cost-effective, and enduring framework using risk management as the underlying basis for security decision making."[2] The Commission views the risk management process as a five-step procedure which they depicted as follows:



The Risk Management Process
Joint Security Commission Model

Looking at this five-step process evokes a sense of *deja vu*, especially for one who knows the five-step risk management process used in operations security! In search of the origin of the version proposed by the Joint Security Commission, contact with a principal writer of this section of the report disclosed the two primary sources which were used for the data: the Central Intelligence Agency's (CIA) Center for Security Evaluations (CSE), and the Interagency OPSEC Support Staff (IOSS). The primary document used from the CSE was a work-in-progress draft instruction being developed for the Overseas Security Policy Group (now the Overseas Security Policy Board (OSPB)) to establish a risk management approach to diplomatic security programs. The OSPB is chaired by the Director, Diplomatic Security Service, Department of State, and has been briefed on operations security by the IOSS.

A comparison of the processes proposed by the Joint Security Commission and the CSE/OSPB with the one the IOSS teaches for operations security, shows more similarities than dissimilarities. Dissimilarities are to be expected in a country where we drive on parkways and park on driveways, send cargo by ship and shipments by rail cars, and establish different standards for the protection of the same information when held by contractors instead of by government agencies. Even the terms used in the report *Redefining Security* to describe the risk management process as a five-step procedure show some variations.

As expected, there are both advocates and opponents of the changes proposed in *Redefining Security*. On 17 June 1994, *A Blueprint for Redefining*

Security was published as a final report by the Joint Security Commission Staff. It described the responses received from the action addressees in the intelligence and defense communities to the eighty-nine (including multipart) recommendations contained in *Redefining Security*, and provided a blueprint for implementing those recommendations. It was noted that *Redefining Security* was received with widespread approval. These are some of the comments highlighted in the report.

> 1. The Department of Energy noted that, "With little exception, this agency is agreeable to the recommendations, and strongly supports them in principle."
>
> 2. The Nuclear Regulatory Commission stated, "Many of the changes proposed...are both practical and overdue."
>
> 3. The Undersecretary of Defense (Policy) said, "We support the majority of the JSC's conclusions and general recommendations," and chose thirty-eight of the Commission's recommendations for "fast track" implementation.
>
> 4. The Deputy Undersecretary of Defense (Acquisition Reform) said, "This Office wholeheartedly endorses the recommendations outlined in the Joint Security Commission's report."
>
> 5. Defense Mapping Agency asserted, "Unquestionably, the recommendations and supporting rationale of the Joint Security Commission provide the greatest opportunity to optimize our security systems."
>
> 6. The Defense Intelligence Agency stated, "The benefits of increased efficiency and productivity improvements [resulting from the Commission's recommendations] should lead to net long-term savings."
>
> 7. And the National Security Agency reported, "The Commission has succeeded in focusing the DoD and intelligence communities on the inconsistencies and excesses in security practices and has offered some excellent recommendations to eliminate duplication, unnecessary spending, and archaic practices."[3]

Of course, despite general agreement with the philosophy expressed in the Commission's *Redefining Security* report, many respondents expressed concern for specific details of the Commission's recommendations, and many offered constructive criticism or alternative recommendations. While the majority of the responses were well-thought out critiques of the entire report, a few responses showed a not-unexpected reluctance to work positively toward the necessary changes in security. Many of the negative responses, given the explanatory text, appear to have been made out of fear of the unknown or a sense of being threatened, especially in this time of declining budgets. A small number of recommendations may have been misunderstood.[4]

What is most interesting is that the single most important concept expressed in *Redefining Security* was not written as a recommendation, but as a statement: "We can and must provide a rational, cost-effective, and enduring framework using risk management as the underlying basis for security decision making."[5] And the proponents of risk management are many.

"In answer to the changing requirements of the 1990s, the CIA is adopting the philosophy of Risk Management, in which the risk of disclosure is weighed against the costs of security practices."[6] Mr. Robert Iwai, then-Director of Security, Central Intelligence Agency, made this statement on May 19, 1993, in an address to the Sixth Annual DoD Security Conference. He cited global instability and diminishing fiscal resources as the catalysts driving a philosophical change in the security arena -- a movement from the philosophy of risk avoidance to risk management. He gave several comparisons between risk management and risk avoidance, summarizing that, "Risk Management is the integrated process of assessing the threat, the vulnerabilities, and the value of the information to the owner." He closed by describing risk management as a flexible, effective, and cost efficient means of implementing security, saying that it "represents progress-it is the vehicle that the CIA is employing to move security into the future and to keep our customers engaged in protecting their information." This certainly constitutes a new paradigm for the CIA. But what of other agencies?

"While many agencies have been practicing 'risk avoidance,' we began using threat based security countermeasures years ago. That is, we have reviewed the threat, analyzed our vulnerabilities, and determined which of those

vulnerabilities our adversaries would most likely have the ability and the will to exploit. I wish to emphasize the pride and appreciation I feel for all of you who have been practicing that which the Joint Security Commission has determined is the best avenue to pursue."[7] These comments were made by Mr. Edward J. McCallum, Director, Safeguards and Security, Department of Energy, in *S&S News and Views* newsletter, January 1994. We can find departments and agencies all along the risk management-avoidance continuum, and all will eventually accept the risk management paradigm proposed by the Joint Security Commission. It will be easier for some than for others.

Risk Management in Other Contexts

The good news is that we in security are not the only community to struggle with the semantics of risk management. In April 1993, a Conference on *The Risk Assessment Paradigm After Ten Years: Policy and Practice Then, Now, and in the Future*, was held at Wright-Patterson AFB, Ohio. It provided an opportunity for research scientists, risk assessment practitioners, and users of risk analysis to evaluate the state of the art of risk assessment. It was noted that the rapid increase in the utilization of risk assessment since the presentation by the National Academy of Sciences (NAS) of an analytical paradigm in 1983[8] had raised numerous and difficult scientific and policy issues. The conference's six sessions addressed *The Basics of Risk Assessment, Case Comparisons - Issues/Lessons Learned, Where the Paradigm Needs Change, Advancing the Science of Risk Assessment (sessions IV and V), and Risk Communication.*[9]

Dorothy E. Patton, Executive Director, Risk Management Forum, Environmental Protection Agency, was one of many who addressed this conference. Writing on the topic of *The NAS Risk Paradigm as a Medium for Communication*, she commented that "Risk assessment is often regarded as confusing, excessively complicated, and needlessly controversial. Indeed, some observers describe it as a 'black box,' a place where government 'hides' policy decisions, or a 'political tool.' Given the complexity, diversity, and uncertainty that characterize both the information content and the practices of risk assessment, such impressions are not surprising." Addressing the NAS paradigm published in 1983, she said that, "As a starting point, perhaps the most useful aspect of the NAS paradigm is its emphasis on defining terms and distinguishing among risk concepts. The paradigm is useful for distinguishing among the several diverse contexts in which risk is analyzed and discussed: risk assessment, risk management, risk communication, risk perception, risk reduction, comparative risk, and relative risk. All embrace risk concepts, all are sometimes used interchangeably, but each has a somewhat different usage."[10] To Ms. Patton's list, we have now added risk avoidance.

A major reason for defining terms and distinguishing among risk concepts is that, without this emphasis, individuals and organizations will define terms to *satisfy their existing paradigms*. As discussed later, some who have worked for years in a traditional security discipline such as physical security think of *threat* only in human or adversarial terms. Others firmly believe that *threat* either exists or it doesn't and, if it does, there is nothing that can be done to mitigate it. *Threat* can be of non-human origin (storms or floods),but human threat, *properly defined and understood*, can be mitigated.

Those who understand the nature of risk and its management in a general sense are more likely to be able to maximize the benefits of risk management in security decision making by applying a *zero- based risk management concept*. It has already been demonstrated that some organizations and agencies are using this new (old) paradigm of risk management only to justify deviations from existing security standards which were usually written from a risk avoidance perspective.

The Interagency Forum for Risk Management Training was established in a meeting of three people on 29 April 1994 with the purpose of trying to find common ground in developing training or other materials relating to risk management and decision making within the security arena. The second meeting, on June 7, was attended by fifteen, and on July 12 a similar number attended searching for the common ground--or at least trying to define what that ground might look like. While the Joint Security Commission urged us to implement the new paradigm--risk management, it is clear that we must first determine what risk management is in a broad context before we can determine how to implement it with some degree of consistency within the somewhat limited arena of security decision making. And we should begin by defining certain terms and distinguishing among risk concepts, beginning with risk, risk assessment, and risk management.

Definitions

Risk management is certainly not a new term or discipline. It has been around for decades. As referenced earlier, the NAS paradigm for managing the process of risk assessment was published in 1983. Its area of application, however, was focused on the characterization of the potential adverse health effects of human exposures to environmental hazards. The Merritt Company, well known in *security*

circles for its **Protection of Assets Manual,** is equally well known in *risk management* circles for its **Risk Management Manual**, advertised as "*The Pro-Active Bible to Risk Management in the 1990's.*" In that manual, first published in 1972 and updated quarterly, the writers currently address **the elusive meaning of risk.** They say that a satisfying definition of **risk** remains **elusive**, but its *characteristics* are well known. While being a relative thing, and a matter of perception, according to the manual, risk always entails the extent to which a person or group *willingly* exposes assets or income to potential loss. One might question whether the *unwilling* but accidental or unavoidable exposure of assets to potential loss eliminates risk. Of course not! So, in search of acceptable definitions, one might turn to a source used every day: a dictionary. And even then, it may be necessary to review more than one dictionary to find definitions that satisfy the research topic.

Risk as a noun is defined as the ***possibility of danger, injury, loss, etc.; the probability of such loss;*** or, as a transitive verb, ***to expose to danger, injury, loss, etc.***[11] Another definition is that risk is the danger or probability of loss to *an insurer*, and *the amount that an insurance company stands to lose.*[12] This is a distinction that raises an important point. ***Risk*** includes not simply the one-dimensional perspective that a loss or injury *may* occur, but also the multi-dimensional perspective of the ***probability*** or ***expectation*** that a loss will occur, and the ***impact*** of that loss. ***Impact*** is the ***amount*** of loss or injury that can be expected. It may be influenced by time or other factors, and may be in terms of dollars, reputation, political consequences, working conditions or operational efficiency or effectiveness.

Assessment is defined as the act, process, or an instance of assessing.[13] **Assess** is to appraise or evaluate.[14] **Appraise** is to evaluate the worth, significance, or status of; especially: to give an *expert judgement* of the value or merit of.[15] The search leads to the listed synonym, "estimate." There, the circle becomes complete with this explanation: **Assess implies a critical appraisal for the purpose of understanding or interpreting, or as a guide in taking action.**[16]

Management is a managing or being managed, such as of a business or other collective enterprise, and **manage** is to exercise control over, or to influence (someone) so that (he/she) does as one wishes.[17]

Incidentally, **"ment"** is a suffix denoting an action or *process*. Also, it should be understood that **risk assessment** is synonymous with **assessment of risk**, and **risk management** is synonymous with **management of risk.** With that, and this brief research of terms, in mind, we should be able to agree with these definitions:

Risk is the probability of danger, injury, or loss to an asset and its impact. (Impact is the amount of loss or injury that can be expected.) It may be influenced by time or other factors, and may be in terms of dollars, reputation, political consequences, working conditions or operational efficiency or effectiveness.

Risk assessment is the process of evaluating threats to and vulnerabilities of an asset to give an expert opinion or calculation on the probability of danger, injury, or loss, and its impact, as a guide in taking action. Impact is the amount of loss or injury that can be expected, as may be influenced by time or other factors.

Risk management is the process of controlling threats to or vulnerabilities of an asset to mitigate the probability of loss or injury or its impact.

Of the three definitions, this last one is usually the most controversial, because some believe that there is nothing that can be done about threat -- it either exists or it doesn't, and, if it does, it cannot be controlled or mitigated by anything that the target of the threat can do. If this is true, our opportunities for managing risk are greatly reduced, being limited to the treatment of vulnerabilities. We must open our minds to the possibility of controlling threat so as to gain the maximum advantage of managing risk. We must place emphasis on defining terms and distinguishing among risk management concepts, just as the scientific community had to do. This will require the modification of some paradigms.

Responsibility for Risk Management

Who is responsible for **risk management?** Many people believe that risk management is the responsibility of management. What has often been misunderstood concerning the division of responsibility **was where** the line should be drawn on this one issue between the security practitioner or team and the customer. The security practitioner or survey team is to offer solutions in the form of appropriate countermeasures, each of which should have been tested by applying the OPSEC or other risk management process.

The purpose of a countermeasure is to exert control over threats, vulnerabilities, or both, in order to mitigate the probability of loss or injury or its impact to the system or operation being surveyed. The security practitioner or survey team is intimately involved in identifying and determining the value of the asset that needs protection; is informed on the threats to the asset (*i.e.*, a system or operation) being surveyed; identifies vulnerabilities of the system or operation; and, considering these factors, assesses the risk to that asset. As the team or

practitioner considers various options for mitigating the risk, they need to test these options to determine whether, or to what degree, they will change the risk; that is, how they will affect the probability of loss or injury or its impact to the system or operation.

As they work this part of the process, they may find themselves discarding some possible solutions as being clearly impractical. For instance, one possible solution for communications vulnerabilities related to "talking around" classified or critical information on unsecured telephones or facsimile machines is to eliminate all unsecured means of communications (telephones and facsimiles). While one effect would be to totally eliminate the specific vulnerability, the adverse impact on the project is highly likely to outweigh the benefits.

Countermeasures

Threat & Vulnerability = Risk. Threat requires both the interest and capability of an adversary to constitute a viable threat. Either of these may be second party issues, such as one party serving the interest of a second to collect against a third party. Vulnerabilities are openings subject to attack. Countermeasures are means by which either threats, or vulnerabilities, or both, may be mitigated. Countermeasures may have different **weights** and **value per unit of weight.** One countermeasure might be to alter the timing of events. Changing the time of some events such as the movement of sensitive material may have little economic impact, but changing the time of major events such as the launching of a space shuttle or a simulated nuclear explosion test can cost hundreds of thousands of dollars. The responsibility of the security practitioner or survey team is to propose **appropriate** countermeasures that bring the balance back to an acceptable level of risk, without undue expense to the customer or impractical or unacceptable burdens on the work force or process.

Allowing free-wheeling brainstorming for countermeasures is often beneficial by looking beyond the obvious, and can help to identify a broader range of options to consider. Using the OPSEC or other risk assessment process to test each option in the same manner that was used for the original conditions helps ensure that options ultimately proposed to the client will be appropriate. Such testing is essential.

Probability of Loss

Remember that the purpose of **risk assessment is to render an expert opinion or calculation** on the probability of loss or injury to a system or operation, and on the expected impact of such a loss or injury. When dealing in probabilities, some people prefer to deal in mathematical calculations to the extent possible. For such customers, it might be appropriate to use mathematical formulas or tools to **calculate** the probability of loss or injury, or the expected impact in terms of the amount of loss or injury that can be expected. For instance, it might be reported that there is a 70% probability of loss of (certain critical information), or the expected loss or damage to a system is $6,000,000, or .8 of the $7,500,000 already committed.

Other people are more comfortable with relative degrees of probability. For these customers, it might be better to render an **expert opinion** in less absolute terms, such as a **Very High, High, Moderate, Low or Very Low** probability of loss (of certain critical information). Or you could say that the expected loss or damage to a system is $6,000,000 of the $7,500,000 already committed, because of the loss of the technological lead that will be compromised by the loss (of the specific critical information). Which of these styles to use should be determined by knowing what will best serve the customer. What is important is to ensure that someone with the requisite skills is available as a member of the survey team to provide the analytic support required for the customer.

It is implicit in the writing of countermeasures that they are proposed or recommended -- and it is implicit if not explicitly discussed with management (the customer) that it remains their prerogative to determine which, if any, countermeasures will be implemented.

Risk Management an Iterative Process

In discussing the JSC depiction of the risk management process, we should agree that the characterization of the process as a five-step procedure does not imply a sequential, but an iterative process. Each step may yield information which affects information developed earlier, requiring appropriate adjustments while the process continues.

Step One

Assess the value of the potential target. This term, used in the depiction of the risk management process, is explained as the first step in the five-step procedure in this way: "*Asset valuation and judgment about consequence of loss.* We determine what is to be protected and appraise its value. Part of asset valuation is understanding that assets may have a value to an adversary that is different from their value to us."[18]

> *Asset* is defined as anything one owns or any quality one has that is of value or use.[19] Within our corporate interests, that may be a

program, system or operation, a specific device or process being developed or manufactured, or the security systems established or implemented to protect other assets. As mentioned in the definition of risk, the amount of loss or injury to an asset may be in terms of dollars, reputation, political consequences, working conditions or operational efficiency or effectiveness.

Step Two

Identify and characterize the threat. This term is explained as the second step of the process in this way: "*Identification and characterization of the threats to specific assets.* Intelligence assessments must address threats to the asset in as much detail as possible, based on the needs of the customer. These assessments may be commissioned at the national level to feed the development of security policies and standards, at the program level to guide systems design, or in planning intelligence support for military or other operations."[20]

> **Threat** is defined as a statement or other indication of intention to hurt, punish, destroy, *etc., or* an indication that an undesirable event or catastrophe may occur, such as *a threat of rain.*[21] The core element in defining threat is not an expressed intent or will, but the indication of potential harm. For our corporate interests, there are two distinct types of threat: human and nature. An expression of intent is to human threat as the lowering of barometric pressure is to an act of nature such as a storm or hurricane threat--an indication of impending danger or harm. Natural events such as hurricanes or earthquakes, which can be real threats, do not have free will but, in some security disciplines, such threats are considered in developing protection plans and in the installation of security systems. However, in most security disciplines, we tend to ignore threats of nature and focus on human threats. In that vein, it is generally believed that to be considered viable (sound, or workable, if translated into action[22]), ***threat*** requires both the will and a capability of the one (individual or group) regarded as a possible danger to exploit a potential target.

This concept has three major flaws.

The first flaw, if one is to remain true to the ***process*** of risk management, and to the ***definition*** of risk, is that one should acknowledge that a threat from *natural events* can cause danger, injury or loss. In that vein, ***threat***, to be viable, must always have a *capability to cause danger, injury or loss, but* ***will*** *or* ***intent to exploit or cause danger, injury, or loss*** is an optional attribute. That is a human attribute which is not always present in a viable threat situation, not even when the origin of the threat is human.

That is the second flaw: the belief that one needs to be a target of exploitation. The observation that one or more participants in a brawl has a handgun can easily be seen as a indication that an undesirable event or catastrophe may occur, and the inadvertent loss of life of an innocent bystander from even the accidental discharge of one of those handguns is predictable, even when the focus of the human participants in the brawl was not upon the bystanders. So, even when the origin of threat is human, there need not be a will to cause danger, injury, or loss, for such a loss to occur. It may be all the more tragic when the person who caused the weapon to fire was simply defending himself, and the weapon did not even belong to him, but the loss is irreversible.

The third flaw is a belief that ***exploitation*** is the only method by which an asset is exposed to danger, injury, or loss. ***Exploit*** means to derive unjust profit, as from the work of another, or to use for one's own selfish ends or profit.[23] While this may be an undesirable event, if it causes no *danger, injury, or loss to an asset* which we wish to protect, we may not care enough to spend our very best efforts on countering this exploitation. On the other hand, we must be sensitive to possible adverse but unforeseen consequences of exploitation. A US manufacturer of light bulbs hosted a visit of foreign

light bulb manufacturers. The US manufacturer was careful to protect the company's new technology of a longer-lasting filament. The foreign manufacturers were interested only in the mechanics of how to blow a better bulb and attach it to a screw base. With the old technology they learned from the US manufacturer, the foreign competitors made, not a better bulb, but a cheaper one, and flooded the US market with cheap five-for-a-dollar bulbs, cutting into the US manufacturer's market share. Similarly, Saddam Hussein was nearly able to field a nuclear weapon capability from old US atomic energy technology gleaned from open source material no longer protected by the US. He is not likely to have cared that his nuclear weapon would have been environmentally "dirty."

For our corporate purpose, we should retain a standard dictionary definition that ***threat*** is an indication that an undesirable event or catastrophe may occur. To be viable, it always requires a capability and, for human threat, *usually* includes the will to cause danger, injury, or loss.

Step Three

Analyze vulnerabilities is explained as the *"Identification and characterization of the vulnerability of specific assets.* Vulnerability assessments help us identify weaknesses in the asset that could be exploited. The manager may then be able to make design or operational changes to reduce risk levels by altering the nature of the asset itself. Cost is an important factor in these decisions, as design changes can be expensive and can impact other mission areas."[24]

The core meaning of **vulnerable** is to be open to attack, *hurt or injury,* or capable of being hurt or wounded, either because insufficiently protected or because sensitive and tender.[25] As explained by the Joint Security Commission, vulnerabilities are weaknesses in the asset that could be exploited. This suggests that **vulnerabilities** are *internal* to the asset. This is not necessarily so--as addressed above, we need to assess the value of the *potential target*--to determine what is to be protected and appraise its value. Exploitable weakness (vulnerabilities) may be in the asset (system or operation) to be protected, such as a covert research and development project, or in the systems or operations intended to protect the asset, such as security systems. Security systems are also assets.

As discussed for threat, however, exploitation is but one means by which an asset may be exposed to danger, injury, or loss. An asset may also be vulnerable by other means, such as inadvertent damage to a system under development.

So, ***vulnerability*** should be defined as an openness to attack or criticism.

Step Four

Identify and cost countermeasures. This is explained as the *"Identification of countermeasures, costs, and tradeoffs.* There may be a number of different countermeasures available to protect an asset, each with varying costs and effectiveness. In many cases, there is a point beyond which adding countermeasures will raise costs without appreciably enhancing the protection afforded."[26]

This appears to be out of place in terms of an analytic process, especially as one reads the JSC explanation of risk assessment, and may contribute to confusion between the risk management process proposed by the Joint Security Commission, and the operations security process contained in the National Operations Security Program. Although the risk management process is an iterative, versus a sequential process, when conducting and reporting on **risk assessments**, the first issue is to assess the risk under existing conditions before implementing any countermeasures. If the existing risk is very low, it may be inappropriate to offer any countermeasures, unless the particular program or project requires a zero percent level of risk.

Once the existing level of risk is established, a variety of countermeasures should be considered and tested by applying

the risk assessment process. This is simply good staff work. Staff officers, consultants, and security survey teams have a responsibility to management that goes beyond identifying problems. They have a responsibility to offer solutions. That is what countermeasures are--solutions. The end purpose of a security survey or assessment is to propose to the customer (the manager or decision maker) certain actions that will lessen the probability of compromise or, in more positive terms, improve the probability that a program or project will succeed, by mitigating either threat(s) or vulnerability(ies) or both. A countermeasure that is not based on a proper risk assessment is conjecture, one synonym for which is **guess**. We should not engage in **guesswork** in the name of security.

Step Five

Assess risks is called *"Risk assessment.* Asset valuation, threat analysis, and vulnerability assessments are considered, along with the acceptable level of risk and any uncertainties, to decide how great is the risk and what countermeasures to apply."[27]

> ***Risk assessment*** *was previously defined as* ***the process of evaluating*** *threats to and vulnerabilities of an asset to give an expert opinion or calculation on the probability of danger, injury, or loss, and its impact, as a guide in taking action. Impact is the amount of loss or injury that can be expected, as may be influenced by time or other factors.*
>
> The security specialist or practitioner, and all the members of a survey team, are responsible for evaluating the threats to and vulnerabilities of a system or operation being surveyed to give an expert opinion or calculation on the probability of danger, injury or loss, and its expected impact to that system or operation, as may be influenced by time or other factors. That is **risk assessment.**
>
> When conducting and reporting on **risk assessments,** the first task is to assess the risk under conditions existing before implementing any countermeasures. If the existing risk is very low, it may be inappropriate to offer any countermeasures, unless the particular program or project requires a zero percent level of risk. While a zero percent level of risk might be nice to have in a nuclear environment, reality is that **if it was achievable,** the cost might well be too high. Even in traditional security fields that have previously focused on risk avoidance, recent changes in the world are forcing security managers and specialists to reorient the disciplines to focus on **managing,** rather than **avoiding,** risks.

Balancing Threats and Vulnerabilities Against Countermeasures

Conceptually, the management of risks with countermeasures might be envisioned as a balance scale. Threats and vulnerabilities each may come in a variety of ways with varying amounts of impact. Together, threats and vulnerabilities constitute risk. The greater the amount of risk, the greater is the need for countermeasures to offset the risk. Countermeasures also may come with varying degrees of impact not necessarily related to costs. A countermeasure of relatively low cost, or one which might result in cost savings, might have a greater impact on risk than a more expensive one. The goal is to reduce risk to an acceptable level at an acceptable cost.

That returns us to the issue of where the line is drawn between the security practitioner or team and the customer concerning responsibility for **risk management**. The team is involved in determining how to exert control over the threats to or vulnerabilities of the asset being surveyed in order to mitigate the probability of loss or injury or its expected impact. By these actions, they are involved in managing the risks to that system or operation. They have a responsibility to go beyond identifying problems. They have a responsibility to offer solutions. Those solutions are in the form of options called countermeasures. It is then the responsibility of the customer--management or a decision maker--to decide which options (countermeasures) to implement. If the team has done its job well, those decisions will be well-informed decisions.

Wiring the World and Risk Management

What does all this have to do with the theme of the *International Security Systems Symposium and*

Exhibition in November 1994?

> "The introduction of the information superhighway has brought tremendous opportunities as well as challenges to business and governments. While allowing for instant access on a global basis to data and information, it has also created major vulnerabilities in protecting proprietary information and technologies. Telephones, computers, corporate board rooms, plants, corporate offices, and military installations are all more easily accessed by unscrupulous individuals, companies, and foreign enemies."

We cannot and should not apply the risk avoidance paradigm of the past to this evolving entrepreneurial environment of opportunities and challenges being found in this new information age. Those who would seek to do well in this new environment must learn to manage the risks they will have to assume concerning how to control access to and release of proprietary or otherwise sensitive information and technologies.

How risk management is implemented will vary with the environment and circumstances within which it is to be implemented. Since the 1980s, "risk management" has become one of the most widely used terms in business. As its use widens, so does its meaning. Insurance brokers mean the proper mix of coverage when they talk about risk management. Pinstriped consultants mean computer-generated financial models. Security people mean control of access, among other things.[28] It is that "control of access, among other things," that we are now exploring with this new (old) paradigm. And control of access to the mass of sensitive data which may be available on the information superhighway, its side roads, and off ramps should be a major concern of those who hope to protect their proprietary information and technologies until they are *ready* to release their data.

Several agencies have been identified as implementing the new (old) paradigm of risk management in redefining their security programs. More will follow. For instance, the one badge concept being implemented within the Department of Energy and its contractor operated facilities is also being explored on a government-wide basis. On-line computer systems are being used for security clearance verification. Need-to-know is no longer considered by many to be just a security issue--the person who has possession of classified matter is expected to exercise control over it, including deciding who else may have access to it. YOUR paradigm on access control is changing--will you change with it?

As previously mentioned, in 1983 the National Academy of Sciences presented an analytical paradigm which, ten years later, became the theme for a conference of *The Risk Assessment Paradigm After Ten Years: Policy and Practice Then, Now, and in the Future.*

In 1988, the then-National Bureau of Standards (NBS) (now the National Institute of Standards and Technology (NIST)) and the National Computer Security Center cooperatively established a Risk Management Research Laboratory at the NBS facilities in Gaithersburg, MD. The primary objective of the laboratory was to conduct research in risk management techniques and methodologies. As part of that endeavor, risk management software products were surveyed to determine their applicability to different agency environments. This resulted in the publication, in March 1992, of *Automated Risk Management Software Tools,* a report which addressed the characteristics of eighteen software products.[29] The NIST is no longer supporting the Risk Management Research Laboratory.

A longer range goal of the Laboratory was to develop and validate a formal framework for analyzing, developing and implementing risk management methods. The intent was to look for methods of risk management which can be economically employed across a broad spectrum of computer environments and upon which standards could be based. NIST is in the process of developing a guideline which describes a number of techniques and methods used in a number of disciplines, such as nuclear energy and transportation, and how those techniques might fit into other environments. This foundation may be readily supportive of broader security risk management needs.

By memorandum dated 10 April 1995, Peter Saderholm, Director, Security Policy Board Staff, proposed the establishment of a Risk Management Working Group to examine formally the issue of risk management. In his memorandum, Mr. Saderholm made the point that the initial step in making risk management the norm for government is to ensure that all agencies have a common understanding of the concept, and that clear and intelligent policy on risk management is also essential. He also pointed out that making risk management a reality rather than a catch phrase will require more than common understanding and clear policy guidance. It will require radical overhaul of the US government security mindset.

The Risk Management Working Group's

proposed purpose will be to develop a thought process or set of principles that program managers could go through in making risk management decisions. It is not to be the task of the working group to champion any particular risk management tools; rather, it will make proposals concerning risk management to the committees under the Security Policy Forum.

This proposal is clearly one whose time has come. As previously stated, the single most important ***concept*** expressed in *Redefining Security* was not written as a recommendation, but as a statement: "We can and must provide a rational, cost-effective, and enduring framework using risk management as the underlying basis for security decision making."[30] As different parts of government have been pursuing this Holy Grail for several decades, perhaps we can now avail ourselves of this historical research and finally achieve this noble goal.

Peter Drucker, a well-known writer on management theory, has said that one problem with planning is that it degenerates into work. We have our work cut out for us.

Calvin A. Wood is an employee of the Department of Energy and Deputy Director of the Interagency OPSEC Support Staff. Comments concerning this article or briefing are invited, and may be sent to the author at the Interagency OPSEC Support Staff, 6411 Ivy Lane, Suite 400, Greenbelt, MD 20770-1405, or faxed to (301) 982-2913.

Footnotes

1 Letter of Jeffrey H. Smith, Chairman, Joint Security Commission, transmitting the report, *Redefining Security*, February 28, 1994.

2 *Redefining Security*, February 28, 1994, Joint Security Commission.

3 Page 2, *A Blueprint for Redefining Security*, June 17, 1994, Joint Security Commission Staff.

4 Page 3, *A Blueprint for Redefining Security*, June 17, 1994, Joint Security Commission Staff.

5 Page 5, *Redefining Security*, February 28, 1994, Joint Security Commission.

6 Presentation by Robert H. Iwai, Sixth Annual DoD Security Conference, May 19, 1993.

7 Edward J. McCallum, Director, Office of Safeguards and Security, Department of Energy, in *S&S News and Views* newsletter, Vol. 1994 No. II.

8 National Research Council, *Risk Assessment in the Federal Government: Managing the Process* (National Academy Press, Washington, D.C., 1983).

9 Society for Risk Analysis, *Risk Analysis, Vol. 14, No. 3, June 1994, Page 217.*

10 Society for Risk Analysis, *Risk Analysis, Vol. 14, No. 3, June 1994, Pages 375-378.*

11 The New Lexicon Webster's Dictionary of the English Language, 1988.

12 Webster's II New Riverside University Dictionary.

13 Webster's Ninth New Collegiate Dictionary.

14 Webster's II New Riverside University Dictionary.

15 Webster's Ninth New Collegiate Dictionary.

16 Webster's Ninth New Collegiate Dictionary.

17 The New Lexicon Webster's Dictionary of the English Language, 1988.

18 Page 5, *Redefining Security*, February 28, 1994.

19 The New Lexicon Webster's Dictionary of the English Language, 1988.

20 Page 5, Redefining Security, February 28, 1994.

21 The New Lexicon Webster's Dictionary of the English Language, 1988.

22 The New Lexicon Webster's Dictionary of the English Language, 1988.

23 The New Lexicon Webster's Dictionary of the English Language, 1988.

24 Page 5, *Redefining Security*, February 28, 1994.

25 The New Lexicon Webster's Dictionary of the English Language, 1988.

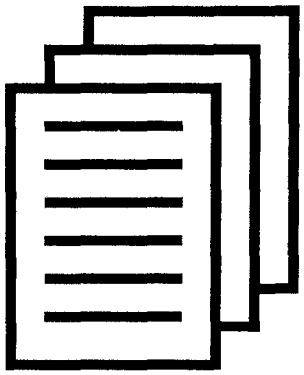
26 Page 5, *Redefining Security*, February 28, 1994.

27 Page 5, *Redefining Security*, February 28, 1994.

28 The Merritt Company, *Risk Management Manual*, February 1993.

29 National Institute of Standards and Technology, *Automated Risk Management Software Tools, March 16, 1992.*

30 Page 5, *Redefining Security*, February 28, 1994, Joint Security Commission.



Executive Order 12968 of August 2, 1995 Access to Classified Information

The national interest requires that certain information be maintained in confidence through a system of classification in order to protect our citizens, our democratic institutions; and our participation within the community of nations. The unauthorized disclosure of information classified in the national interest can cause irreparable damage to the national security and loss of human life.

Security policies designed to protect classified information must ensure consistent, cost effective, and efficient protection of our Nation's classified information, while providing fair and equitable treatment to those Americans upon whom we rely to guard our national security.

This order establishes a uniform Federal personnel security program for employees who will be considered for initial or continued access to classified information.

NOW, THEREFORE, by the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

PART 1 - DEFINITIONS, ACCESS TO CLASSIFIED INFORMATION, FINANCIAL DISCLOSURE, AND OTHER ITEMS

Section 1.1. *Definitions. For the purposes of this order:*

(a) "Agency" means any "Executive agency," as defined in 5 U.S.C. 105, the "military departments," as defined in 5 U.S.C. 102, and any other entity within the executive branch that comes into the possession of classified information, including the Defense Intelligence Agency, National Security Agency, and the National Reconnaissance Office.

(b) "Applicant" means a person other than an employee who has received an authorized conditional offer of employment for a position that requires access to classified information.

(c) "Authorized investigative agency" means an agency authorized by law or regulation to conduct a counterintelligence investigation or investigation of persons who are proposed for access to classified information to ascertain whether such persons satisfy the criteria for obtaining and retaining access to such information.

(d) "Classified information" means information that has been determined pursuant to Executive Order No. 12958, or any successor order, Executive Order No. 12951, or any successor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011), to require protection against unauthorized disclosure.

(e) "Employee" means a person, other than the President and Vice President, employed by, detailed or assigned to, an agency, including members of the Armed Forces; an expert or consultant to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of an agency, including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of any agency as determined by the appropriate agency head.

(f) "Foreign power" and "agent of a foreign power" have the meaning provided in 50 U.S.C. 1801.

(g) "Need for access" means a determination that an employee requires access to a particular level of classified information in order to perform or assist in a lawful and authorized governmental function.

(h) "Need-to-know" means a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

(i) "Overseas Security Policy Board" means the Board established by the President to consider, develop, coordinate and promote policies, standards and agreements on overseas security operations, programs and projects that affect all United States Government agencies under the authority of a Chief of Mission.

(j) "Security Policy Board" means the Board established by the President to consider, coordinate, and recommend policy directives for U.S. security policies, procedures, and practices.

(k) "Special access program" has the meaning provided in section 4.1 of Executive Order No. 12958, or any successor order.

Section. 1.2. *Access to Classified Information:*

(a) No employee shall be granted access to classified information unless that employee has been determined to be eligible in accordance with this order and to possess a need-to-know.

(b) Agency heads shall be responsible for establishing and maintaining an effective program to ensure that access to classified information by each employee is clearly consistent with the interests of the national security.

(c) Employees shall not be granted access to classified information unless they:

> (1) have been determined to be eligible for access under section 3.1 of this order by agency heads or designated officials based upon a favorable adjudication of an appropriate investigation of the employee's background;
>
> (2) have a demonstrated need-to-know; and
>
> (3) have signed an approved nondisclosure agreement.

(d) All employees shall be subject to investigation by an appropriate government authority prior to being granted access to classified information and at any time during the period of access to ascertain whether they continue to meet the requirements for access.

(e)(1) All employees granted access to classified information shall be required as a condition of such access to provide to the employing agency written consent permitting access by an authorized investigative agency, for such time as access to classified information is maintained and for a period of 3 years thereafter, to;

> (A) relevant financial records that are maintained by a financial institution as defined in 31 U.S.C. 5312(a) or by a holding company as defined in section 1101(6) of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401);
>
> (B) consumer reports pertaining to the employee under the Fair Credit Reporting Act (15 U.S.C. 1681a); and
>
> (C) records maintained by commercial entities within the United States pertaining to any travel by the employee outside the United States.

(2) Information may be requested pursuant to employee consent under this section where;

> (A) there are reasonable grounds to believe, based on credible information, that the employee or former employee is, or may be, disclosing classified information in an unauthorized manner to a foreign power or agent of a foreign power;
>
> (B) information the employing agency deems credible indicates the employee or former employee has incurred excessive indebtedness or has acquired a level of affluence that cannot be explained by other information; or
>
> (C) circumstances indicate the employee or former employee had the capability and opportunity to disclose classified information that is known to have been lost or compromised to a foreign power or an agent of a foreign power.

(3) Nothing in this section shall be construed to affect the authority of an investigating agency to obtain information pursuant to the Right to Financial Privacy Act, the Fair Credit Reporting Act or any other applicable law.

Section 1.3. *Financial Disclosure.*

(a) Not later than 180 days after the effective date of this order, the head of each agency that originates, handles, transmits, or possesses classified information shall designate each employee, by position or category where possible, who has a regular need for access to classified information that, in the discretion of the agency head, would reveal:

> (1) the identity of covert agents as defined in the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421);
>
> (2) technical or specialized national intelligence collection and processing systems that, if disclosed in an unauthorized manner, would substantially negate or impair the effectiveness of the system;
>
> (3) the details of:
>
> > (A) the nature, contents, algorithm, preparation, or use

of any code, cipher, or cryptographic system or;

(B) the design, construction, functioning, maintenance, or repair of any cryptographic equipment; but not including information concerning the use of cryptographic equipment and services;

(4) particularly sensitive special access programs, the disclosure of which would substantially negate or impair the effectiveness of the information or activity involved; or

(5) especially sensitive nuclear weapons design information (but only for those positions that have been certified as being of a high degree of importance or sensitivity, as described in section 145(f) of the Atomic Energy Act of 1954, as amended).

(b) An employee may not be granted access, or hold a position designated as requiring access, to information described in subsection (a) unless, as a condition of access to such information, the employee:

(1) files with the head of the agency a financial disclosure report, including information with respect to the spouse and dependent children of the employee, as part of all background investigations or reinvestigations;

(2) is subject to annual financial disclosure requirements, if selected by the agency head; and

(3) files relevant information concerning foreign travel, as determined by the Security Policy Board.

(c) Not later than 180 days after the effective date of this order, the Security Policy Board shall develop procedures for the implementation of this section, including a standard financial disclosure form for use by employees under subsection (b) of this section, and agency heads shall identify certain employees, by position or category, who are subject to annual financial disclosure.

Section 1.4. *Use of Automated Financial Record Data Bases.* As part of all investigations and reinvestigations described in section 1.2(d) of this order, agencies may request the Department of the Treasury, under terms and conditions prescribed by the Secretary of the Treasury, to search automated data bases consisting of reports of currency transactions by financial institutions, international transportation of currency or monetary instruments, foreign bank and financial accounts, transactions under $10,000 that are reported as possible money laundering violations, and records of foreign travel.

Section 1.5. *Employee Education and Assistance.* The head of each agency that grants access to classified information shall establish a program for employees with access to classified information to:

(a) educate employees about individual responsibilities under this order; and

(b) inform employees about guidance and assistance available concerning issues that may affect their eligibility for access to classified information, including sources of assistance for employees who have questions or concerns about financial matters, mental health, or substance abuse.

PART 2 - ACCESS ELIGIBILITY POLICY AND PROCEDURE

Section 2.1. *Eligibility Determinations.*

(a) Determinations of eligibility for access to classified information shall be based on criteria established under this order. Such determinations are separate from suitability determinations with respect to the hiring or retention of persons for employment by the government or any other personnel actions.

(b) The number of employees that each agency determines are eligible for access to classified information shall be kept to the minimum required for the conduct of agency functions.

(1) Eligibility for access to classified information shall not be requested or granted solely to permit entry to, or ease of movement within, controlled areas when the employee has no need for access, and access to classified information may reasonably be prevented.

Where circumstances indicate employees may be inadvertently exposed to classified information in the course of their duties, agencies are authorized to grant or deny, in their discretion, facility access approvals to such employees based on an appropriate level of investigation as determined by each agency.

(2) Except in agencies where eligibility for access is a mandatory condition of employment, eligibility for access to classified information shall only be requested or granted based on a demonstrated, foreseeable need for access. Requesting or approving eligibility in excess of actual requirements is prohibited.

(3) Eligibility for access to classified information may be granted where there is a temporary need for access, such as one-time participation in a classified project, provided the investigative standards established under this order have been satisfied, in such cases, a fixed date or event for expiration shall be identified and access to classified information shall be limited to information related to the particular project or assignment.

(4) Access to classified information shall be terminated when an employee no longer has a need for access.

Section 2.2. *Level of Access Approval.*

(a) The level at which an access approval is granted for an employee shall be limited, and relate directly, to the level of classified information for which there is a need for access. Eligibility for access to a higher level of classified information includes eligibility for access to information classified at a lower level.

(b) Access to classified information relating to a special access program shall be granted in accordance with procedures established by the head of the agency that created the program or, for programs pertaining to intelligence activities (including special activities but not including military operational, strategic, and tactical programs) or intelligence sources and methods, by the Director of Central Intelligence. To the extent possible and consistent with the national security interests of the United States, such procedures shall be consistent with the standards and procedures established by and under this order.

Section 2.3. *Temporary Access to Higher Levels.*

(a) An employee who has been determined to be eligible for access to classified information based on favorable adjudication of a completed investigation may be granted temporary access to a higher level where security personnel authorized by the agency head to make access eligibility determinations find that such access:

(1) is necessary to meet operational or contractual exigencies not expected to be of a recurring nature;

(2) will not exceed 180 days; and

(3) is limited to specific, identifiable information that is made the subject of a written access record.

(b) Where the access granted under subsection (a) of this section involves another agency's classified information, that agency must concur before access to its information is granted.

Section 2.4. *Reciprocal Acceptance of Access Eligibility Determinations.*

(a) Except when an agency has substantial information indicating that an employee may not satisfy the standards in section 3.1 of this order, background investigations and eligibility determinations conducted under this order shall be mutually and reciprocally accepted by all agencies.

(b) Except where there is substantial information indicating that the employee may not satisfy the standards in section 3.1 of this order, an employee with existing access to a special access program shall not be denied eligibility for access to another special access program at the same sensitivity level as determined personally by the agency head or deputy agency head, or have an existing access eligibility readjudicated, so long as the employee has a need for access to the information involved.

(c) This section shall not preclude agency heads from establishing additional, but not duplicate, investigative or adjudicative procedures for a special access program or for candidates for detail or assignment to their agencies, where such procedures are required in exceptional circumstances to protect the national security.

(d) Where temporary eligibility for access is granted

under sections 2.3 or 3.3 of this order or where the determination of eligibility for access is conditional, the fact of such temporary or conditional access shall be conveyed to any other agency that considers affording the employee access to its information.

Section 2.5. *Specific Access Requirement.*

(a) Employees who have been determined to be eligible for access to classified information shall be given access to classified information only where there is a need-to-know that information.

(b) It is the responsibility of employees who are authorized holders of classified information to verify that a prospective recipient's eligibility for access has been granted by an authorized agency official and to ensure that a need-to-know exists prior to allowing such access, and to challenge requests for access that do not appear well-founded.

Section 2.6. *Access by Non-United States Citizens.*

(a) Where there are compelling reasons in furtherance of an agency mission, immigrant alien and foreign national employees who possess a special expertise may, in the discretion of the agency, be granted limited access to classified information only for specific programs, projects, contracts, licenses, certificates, or grants for which there is a need for access. Such individuals shall not be eligible for access to any greater level of classified information than the United States Government has determined may be releasable to the country of which the subject is currently a citizen, and such limited access may be approved only if the prior 10 years of the subject's life can be appropriately investigated. If there are any doubts concerning granting access, additional lawful investigative procedures shall be fully pursued.

(b) Exceptions to those requirements may be permitted only by the agency head or the senior agency official designated under section 6.1 of this order to further substantial national security interests.

PART 3 - ACCESS ELIGIBILITY STANDARDS

Section 3.1. *Standards.*

(a) No employee shall be deemed to be eligible for access to classified information merely by reason of Federal service or contracting, licensee, certificate holder, or grantee status, or as a matter of right or privilege, or as a result of any particular title, rank, position, or affiliation.

(b) Except as provided in sections 2.6 and 3.3 of this order, eligibility for access to classified information shall be granted only to employees who are United States citizens for whom an appropriate investigation has been completed and whose personal and professional history affirmatively indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of classified information. A determination of eligibility for access to such information is a discretionary security decision based on judgments by appropriately trained adjudicative personnel. Eligibility shall be granted only where facts and circumstances indicate access to classified information is clearly consistent with the national security interests of the United States, and any doubt shall be resolved in favor of the national security.

(c) The United States Government does not discriminate on the basis of race, color, religion, sex, national origin, disability, or sexual orientation in granting access to classified information.

(d) In determining eligibility for access under this order, agencies may investigate and consider any matter that relates to the determination of whether access is clearly consistent with the interests of national security. No inference concerning the standards in this section may be raised solely on the basis of the sexual orientation of the employee.

(e) No negative inference concerning the standards in this section may be raised solely on the basis of mental health counseling. Such counseling can be a positive factor in eligibility determinations. However, mental health counseling, where relevant to the adjudication of access to classified information, may justify further inquiry to determine whether the standards of subsection (b) of this section are satisfied, and mental health may be considered where it directly relates to those standards.

(f) Not later than 180 days after the effective date of this order, the Security Policy Board shall develop a common set of adjudicative guidelines for determining eligibility for access to classified information, including access to special access programs.

Section 3.2. *Basis for Eligibility Approval.*

(a) Eligibility determinations for access to classified information shall be based on information concerning the applicant or employee that is acquired through the investigation conducted pursuant to this order or otherwise available to security officials and shall be made part of the

applicant's or employee's security record. Applicants or employees shall be required to provide relevant information pertaining to their background and character for use in investigating and adjudicating their eligibility for access.

(b) Not later than 180 days after the effective date of this order, the Security Policy Board shall develop a common set of investigative standards for background investigations for access to classified information. These standards may vary for the various levels of access.

(c) Nothing in this order shall prohibit an agency from utilizing any lawful investigative procedure in addition to the investigative requirements set forth in this order and its implementing regulations to resolve issues that may arise during the course of a background investigation or reinvestigation.

Section 3.3. *Special Circumstances.*

(a) In exceptional circumstances where official functions must be performed prior to the completion of the investigative and adjudication process, temporary eligibility for access to classified information may be granted to an employee while the initial investigation is underway. When such eligibility is granted, the initial investigation shall be expedited.

(1) Temporary eligibility for access under this section shall include a justification, and the employee must be notified in writing that further access is expressly conditioned on the favorable completion of the investigation and issuance of an access eligibility approval. Access will be immediately terminated, along with any assignment requiring an access eligibility approval, if such approval is not granted.

(2) Temporary eligibility for access may be granted only be security personnel authorized by the agency head to make access eligibility determinations and shall be based on minimum investigative standards developed by the Security Policy Board not later than 180 days after the effective date of this order.

(3) Temporary eligibility for access may be granted only to particular, identified categories of classified information necessary to perform the lawful and authorized functions that are the basis for the granting of temporary access.

(b) Nothing in subsection (a) shall be construed as altering the authority of an agency head to waive requirements for granting access to classified information pursuant to statutory authority.

(c) Where access has been terminated under section 2.1(b)(4) of this order and a new need for access arises, access eligibility up to the same level shall be reapproved without further investigation as to employees who were determined to be eligible based on a favorable adjudication of an investigation completed within the prior 5 years, provided they have remained employed by the same employer during the period in question, the employee certifies in writing that there has been no change in the relevant information provided by the employee for the last background investigation, and there is no information that would tend to indicate the employee may no longer satisfy the standards established by this order for access to classified information.

(d) Access eligibility shall be reapproved for individuals who were determined to be eligible based on a favorable adjudication of an investigation completed within the prior 5 years and who have been retired or otherwise separated from the United States Government employment for not more than 2 years; provided there is no indication the individual may no longer satisfy the standards of this order, the individual certifies in writing that there has been no change in the relevant information provided by the individual for the last background investigation, and an appropriate record check reveals no unfavorable information.

Section 3.4. *Reinvestigation Requirements.*

(a) Because circumstances and characteristics may change dramatically over time and thereby alter the eligibility of employees for continued access to classified information, reinvestigations shall be conducted with the same priority and care as initial investigations.

(b) Employees who are eligible for access to classified information shall be the subject of periodic reinvestigations and may also be reinvestigated if, at any time, there is reason to believe that they may no longer meet the standards for access established in this order.

(c) Not later than 180 days after the effective date of this order, the Security Policy Board shall develop a common set of reinvestigative standards, including the frequency of reinvestigations.

PART 4 - INVESTIGATIONS FOR FOREIGN GOVERNMENTS

Section 4. *Authority.*

Agencies that conduct background investigations, including the Federal Bureau of Investigation and the Department of State, are authorized to conduct personnel security investigations in the United States when requested by a foreign government as part of its own personnel security program and with the consent of the individual.

PART 5 - REVIEW OF ACCESS DETERMINATIONS

Section. 5.1. *Determinations of Need for Access.*

A determination under section 2.1(b)(4) of this order that an employee does not have, or no longer has a need for access is a discretionary determination and shall be conclusive.

Section. 5.2. *Review Proceedings for Denials or Revocations of Eligibility for Access.*

(a) Applicants and employees who are determined to not meet the standards for access to classified information established in section 3.1 of this order shall be:

(1) provided as comprehensive and detailed a written explanation of the basis for that conclusion as the national security interests of the United States and other applicable law permit;

(2) provided within 30 days, upon request and to the extent the documents would be provided if requested under the Freedom of Information Act [5 U.S.C. 552] or the Privacy Act [3 U.S.C. 552a], as applicable, any documents, records, and reports upon which a denial or revocation is based;

(3) informed of their right to be represented by counsel or other representative at their own expense; to request any documents, records, and reports as described in section 5.2(a)(2) upon which a denial or revocation is based; and to request the entire investigative file, as permitted by the national security and other applicable law, which, if requested, shall be promptly provided prior to the time set for a written reply;

(4) provided a reasonable opportunity to reply in writing to, and to request a review of, the determination;

(5) provided written notice of and reasons for the results of the review, the identity of the deciding authority, and written notice of the right to appeal;

(6) provided an opportunity to appeal in writing to a high level panel, appointed by the agency head, which shall be comprised of at least three members, two of whom shall be selected from outside the security field. Decisions of the panel shall be in writing, and final except as provided in subsection (b) of this section; and

(7) provided an opportunity to appear personally and to present relevant documents, materials, and information at some point in the process before an adjudicative or other authority, other than the investigating entity, as determined by the agency head. A written summary or recording of such appearance shall be made part of the applicant's or employee's security record, unless such appearance occurs in the presence of the appeals panel described in subsection (a)(6) of this section.

(b) Nothing in this section shall prohibit an agency head from personally exercising the appeal authority in subsection (a)(6) of this section based upon recommendations from an appeals panel. In such case, the decision of the agency head shall be final.

(c) Agency heads shall promulgate regulations to implement this section and, at their sole discretion and as resources and national security considerations permit, may provide additional review proceedings beyond those required by subsection (a) of this section. This section does not require additional proceedings, however, and creates no procedural or substantive rights.

(d) When the head of an agency or principal deputy personally certifies that a procedure set forth in this section cannot be made available in a particular case without damaging the national security interests of the United States by revealing classified

information, the particular procedure shall not be made available. This certification shall be conclusive.

(e) This section shall not be deemed to limit or affect the responsibility and power of an agency head pursuant to any law or other Executive order to deny or terminate access to classified information in the interests of national security. The power and responsibility to deny or terminate access to classified information pursuant to any law or other Executive order may be exercised only where the agency head determines that the procedures prescribed in subsection (a) of this section cannot be invoked in a manner that is consistent with national security. This determination shall be conclusive.

(f)(1) This section shall not be deemed to limit or affect the responsibility and power of an agency head to make determinations of suitability for employment.

(2) Nothing in this section shall require that an agency provide the procedures prescribed in subsection (a) of this section to an applicant where a conditional offer of employment is withdrawn for reasons of suitability or any other reason other than denial of eligibility for access to classified information.

(3) A suitability determination shall not be used for the purpose of denying an applicant or employee the review proceedings of this section where there has been a denial of revocation of eligibility for access to classified information.

PART 6 - IMPLEMENTATION

Section. 6.1. *Agency Implementing Responsibilities.*

Heads of agencies that grant employees access to classified information shall:

(a) designate a senior agency official to direct and administer the agency's personnel security program established by this order. All such programs shall include active oversight and continuing security education and awareness programs to ensure effective implementation of this order;

(b) cooperate, under the guidance of the Security Policy Board, with other agencies to achieve practical, consistent, and effective adjudicative training and guidelines; and

(c) conduct periodic evaluations of the agency's implementation and administration of this order, including the implementation of section 1.3(a) of this order. Copies of each report shall be provided to the Security Policy Board.

Section 6.2. *Employee Responsibilities.*

(a) Employees who are granted eligibility for access to classified information shall:

(1) protect classified information in their custody from unauthorized disclosure;

(2) report all contacts with persons, including foreign nationals, who seek in any way to obtain unauthorized access to classified information;

(3) report all violations of security regulations to the appropriate security officials; and

(4) comply with all other security requirements set forth in this order and its implementing regulations.

(b) Employees are encouraged and expected to report any information that raises doubts as to whether another employee's continued eligibility for access to classified information is clearly consistent with the national security.

Section. 6.3. *Security Policy Board Responsibilities and Implementation.*

(a) With respect to actions taken by the Security Policy Board pursuant to sections 1.3(c), 3.1(f), 3.2(b), 3.3(a)(2),and 3.4(c) of this order, the Security Policy Board shall make recommendations to the President through the Assistant to the President for National Security Affairs for implementation.

(b) Any guidelines, standards, or procedures developed by the Security Policy Board pursuant to this order shall be consistent with those guidelines issued by the Federal Bureau of Investigation in March 1994 on Background Investigations Policy/ Guidelines Regarding Sexual Orientation.

(c) In carrying out its responsibilities under this order, the Security Policy Board shall consult where appropriate with the Overseas Security Policy Board. In carrying out its responsibilities under section 1.3(c) of this order, the Security Policy Board shall obtain the concurrence of the Director of the Office of Management and Budget.

Section 6.4. *Sanctions.*

Employees shall be subject to appropriate sanctions if they knowingly and willfully grant eligibility for, or allow access to, classified information in violation

of this order or its implementing regulations. Sanctions may include reprimand, suspension without pay, removal, and other actions in accordance with applicable law and agency regulations.

PART 7 - GENERAL PROVISIONS

Section 7.1. *Classified Information Procedures Act.*

Nothing in this order is intended to alter the procedures established under the Classified Information Procedures Act (18 U.S.C. App. 1).

Section 7.2. *General.*

(a) Information obtained by an agency under sections 1.2(e) or 1.3 of this order may not be disseminated outside the agency, except to:

(1) the agency employing the employee who is the subject of the records or information;

(2) the Department of Justice for law enforcement or counterintelligence purposes; or

(3) any agency if such information is clearly relevant to the authorized responsibilities of such agency.

(b) The Attorney General, at the request of the head of an agency, shall render an interpretation of this order with respect to any question arising in the course of its administration.

(c) No prior Executive orders are repealed by this order. To the extent that this order is inconsistent with any provision of any prior Executive order, this order shall control, except that this order shall not diminish or otherwise affect the requirements of Executive Order No. 10450, the denial and revocation procedures provided to individuals covered by Executive Order No. 10865, as amended, or access by historical researchers and former presidential appointees under Executive Order No. 12958 or any successor order.

(d) If any provision of this order or the application of such provision is held to be invalid, the remainder of this order shall not be affected.

(e) This Executive order is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right to administrative or judicial review, or any other right or benefit or trust responsibility, substantive or procedural, enforceable by a party against the United States, its agencies or instrumentalities, its officers or employees, or any other person.

(f) This order is effective immediately.

THE WHITE HOUSE
August 2, 1995