September 1991/Number 2-91

security awareness bulletin

Inside:

AIS Security

Department of Defense Security Institute, Richmond, Virginia

security awareness bulletin

Approved for open publication — Unlimited reproduction authorized

Director
Department of Defense Security Institute
R. Everett Gravelle

Editor
Lynn Fischer

Staff Writer
Tracy Gulledge

The *Security Awareness Bulletin* is produced by the Department of Defense Security Institute, Educational Programs Department, c/o Defense General Supply Center, Richmond Virginia 23297-5091; (804) 275-3824/4223, Autovon 695-3824/4223. Primary distribution is to DoD components and contractors cleared for classified access under the Defense Industrial Security Program and Special Access Programs. Our purpose is to promote security awareness and compliance with security procedures through dissemination of information to security trainers regarding current security and counterintelligence developments, training aids, and educational methods as well as through distribution of textual material for direct training application.

Administrative inquiries, new distribution, address changes: please refer as follows:

Army activities: HQ DA (DAMI-CIS), Washington, DC 20310

Navy & Marine Corps: Security Policy Div (OP-09N), Washington, DC 20350

Air Force: Headquarters AFOSP/SPIB, Kirtland AFB, NM 87117

DIS activities: HQ DIS/V0954

DISP contractors: Cognizant Security Office

Other government agencies: Headquarters security education office

The Threat to Automated Data Systems

by Dr. Lynn F. Fischer, Chief, Security Awareness Division
Department of Defense Security Institute

An article in the Security Awareness Bulletin of June, 1986, was entitled "Real or Imagined? The Hostile Intelligence Threat to Computer Systems." That report stated that while we could cite no examples of known foreign intelligence efforts to steal sensitive and classified information from our computer systems, we had every reason to believe that foreign intelligence services were trying.

There was in fact, by 1986, one alleged exploitation of U.S. data bases by the Soviets openly reported by the press. This was said to have been done through a Vienna-based research institute which employed both Western and Soviet-bloc scientists. Computer networking facilities at the institute provided Soviet scientists with an open invitation to tap into unclassified (but sensitive) defense-related data bases maintained by the United States government. Furthermore, as the article pointed out, the outrageous success that teen-age computer hackers were having in breaking into restricted government data networks with their home computers and modems led to the reasonable conclusion that foreign agents could easily be doing the same thing. As that piece prophetically stated, "If these kids can do it...why can't the KGB do it?"

The German Computer Spy Ring

Our fears were soon confirmed. Reports surfaced of a mysterious break-in through a telephone link at the Lawrence Berkeley Laboratory in California. A 75 cent discrepancy in the accounting summary for on-line charges indicated access to the system by an unauthorized user—a breach in security. Through the persistence of Dr. Clifford Stoll, a system administrator employed at Berkeley, an FBI inquiry was launched in late 1986. Stoll had also been contacted earlier by a systems administrator at the National Security Agency because of several unsuccessful attempts, by a user on the Berkeley system, to enter the NSA computer. Since the intruders had not attempted to destroy files and had attacked exclusively military, nuclear, and defense contractor sites, it was evident that this was some type of espionage operation. After weeks of painstaking tracing and monitoring of attempts to penetrate at least 200 other systems, Stoll, working with systems administrators at other sites, eventually followed the hacker's path to Europe.

The criminal investigation carried out by U.S. and German authorities resulted in the identification and arrest of three West German computer hackers in Hamburg in March 1989.* At the time of their arrest, authorities announced that the trio had received several thousand dollars from the KGB for diskettes containing sensitive data from data banks at the Pentagon, Los Alamos National Laboratory and NASA. Penetration of several other computer databases in Western Europe was also suspected.

When you come to think about it, this event was just as much a classic espionage case as that of John Walker, Jonathan Pollard, or James Hall—except that the methods and technology of the perpetrators were different. In all of these, sensitive, defense-related information was illegally obtained in exchange for money by a foreign interest for the purpose of military or technological advantage.

Masters of Doom

Foreign intelligence services and industrial interests are not the only threat to sensitive, automated systems and databases. Extensive economic damage has in fact resulted from the activities of hackers who appear to be motivated by a sense of intrigue, intellectual challenge and gamesmanship.

One of the most alarming penetrations of defense computer systems occurred in 1987 when a 17-year old Chicago hacker, Herbert Zinn, who went by the alias of Shadow Hawk, was brought to trial for the unauthorized theft of software files from Bell Laboratories, the U.S. Missile Command System, and Robbins Air Force Base. He is reported to have illegally copied software valued at more that $1.2 million including complex programs on artificial intelligence and computer design regarded by the U.S. government as "highly sensitive." Zinn actually went to the extent of placing his break-in methods on bulletin boards and encouraging others to try the same thing. Although claiming he did this for educational purposes, Zinn, the first hacker convicted under the Computer Fraud and Abuse Act of 1986, received a $10,000 fine and a 9-month jail sentence.

Teen-age assaults on Department of Defense systems have not abated. As reported in the press in November 1989, a New York high school student who used the name

* For a full account of this case read *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage*, by Clifford Stoll, Doubleday, New York, NY 1989. Also related to this case study is the slide-text briefing package, "The Adventures of an Overseas Hacker," advertised in this copy of the *Bulletin*.

of "Zod" broke into the Pentagon office system of the Secretary of the Air Force. This penetration, which "crashed" the system, was reported in the press to have required $250,000 to repair. Although (according to a senior investigator in the New York State Police) no national security information was compromised, an Air Force spokesman admitted that the system contained information that was "sensitive in aggregate; if you had information on A and B and C from the system, put it together, and you have F—sensitive information of interest to parties outside the government." This, in fact, is a very succinct explanation of why we need to be very concerned about the fact that defense-related networks can be accessed by unauthorized users even though they may not contain formally classified information. Zod, by the way, was a 14-year old member of the MOD (Masters of Doom) hackers club, a successor group to the Legion of Doom which had caused similar havoc in the late 1980s.

Hacking with Impunity

Although several cases of illegal access through telephone links in this country and in Germany have been successfully prosecuted, the absence of standard computer crime laws in Europe has made it possible for hackers to penetrate U.S. computer networks by long-distance phone from several other locations. This past April a story in the *New York Times* described how Dutch hackers broke into U.S. military systems while being filmed by a Dutch television station. According to the news report, while it was claimed by Federal authorities that no serious damage was done, the group successfully entered and browsed through systems at the Kennedy Space Center, the Pacific Fleet Command, and Lawrence Livermore National Laboratory via *Internet*, an international data communications network.

Is this just the visible tip of the iceberg? How many "sensitive systems," as defined by the Computer Security Act of 1987, are being subject to illegal access due to inadequate controls? According to a General Accounting Office report issued in January 1990, one such network for scientific information maintained by NASA has been repeatedly violated over the past ten years by unauthorized users at domestic and overseas locations. Due to design and management weakness in the Space Physics Analysis Network (SPAN), scores of unauthorized users were allowed to browse through and copy technical files for the past decade. Part of the problem, according to the GAO report, is that the Goddard Space Flight Center which maintains the network, delegated user approval and security management to local management at each of the 6,000 nodes in the network. With reference to what might have been lost, no amount of value could be placed on the technical and design information obtained by potential adversary nations.

Stealing Classified Documents?

As we go to press with this issue, three men stand indicted for gaining illegal access to the Army MASNET Computer Network and of having obtained Secret files about a military exercise at Fort Bragg N.C. and FBI case files in early 1987. According to information provided at a press conference by U.S. Attorney Joseph Russoniello in San Francisco, while the information has since been declassified, this possible theft alerts us to serious vulnerabilities in defense system computers.

The men are alleged to have (physically) broken into Pacific Bell Telephone sites to steal access codes and telecommunications equipment which allowed them to get into the MASNET system. While the indictment does not indicate what their ultimate intent was, it is known that one of the individuals is accused of also obtaining the unlisted telephone numbers for the Soviet Consulate in San Francisco by the same methods. As a teenager he was known as a notorious computer hacker by the name of Dark Dante. Dark Dante, at the age of 17, was an unindicted co-conspirator in a computer system break-in at the University of California at Los Angeles in 1984.

Computer Sabotage and the Insider Threat

There are, of course, other reasons, in addition to countering espionage and gamesmanship why security countermeasures are employed in automated environments. Electronically stored text and quantitative data must be safeguarded from individuals who would attempt to alter or destroy it for illegal profit, revenge, or even ego gratification. In the past several years there have been numerous attempts reported in the private sector to corrupt or block legitimate access to critical files by vindictive employees. For example, in the first successful prosecution of its type, Donald Burleson, a former computer programmer at an insurance firm in Fort Worth was convicted of computer sabotage for planting a virus which wiped out 168,000 payroll records two days after he was fired. Burleson had been sacked because of repeated conflicts with co-workers.

Somewhat closer to home is the case of a San Diego computer programmer alleged to have planted a logic bomb* in the mainframe system of General Dynamics, one of our largest defense contractors. In June 1991 felony charges were brought against the former employee for computer fraud and computer tampering. The individual had resigned from the company in March due to, in his opinion, lack of recognition and is alleged to have installed the "bomb," set to go off over the Memorial Day weekend.

*A logic bomb is a type of Trojan Horse which is set to go off at a certain time or when specific conditions are met. See the accompanying article on viruses in this issue.

Agent William Landreth of the Defense Criminal Investigative Service stated, "This is the most egregious attempted computer sabotage I've seen because it involved a person in a position of trust." According to Landreth, the bomb could have cost more than $100,000 in reprogramming and would have destroyed irreplaceable data on General Dynamics contracts, including the Atlas Missile Space Program. Fortunately the bomb or "Trojan horse" was detected and disarmed by another employee before "scheduled detonation," according to a *San Diego Tribune* report.

Virus Attacks

Under the category of total systemic attack is the recent case of Robert Tappan Morris a computer science graduate student at Cornell university. In January 1990 Morris was convicted under the 1986 Computer Fraud and Abuse Act of infecting a nation-wide network with a virus which virtually shut down an entire network of 6,000 UNIX-based computers. As discussed elsewhere in this issue of the *Bulletin*, viruses are programming codes that attach themselves to legitimate programs and files, then reproduce themselves and spread by diskette or remote down-loading to other computers or networks. Their effects range from unexpected messages to total destruction of files and programs.

Morris' offense was dubbed the "INTERNET Worm Case" since his contagious code was transmitted via the INTERNET network and did not have to attach itself to another program in order to spread and duplicate itself. In fact, the worm replicated wildly and seriously affected operations at several top government and academic computer centers in late 1988. Systems affected included Stanford and Columbia Universities, the Lawrence Livermore Laboratory, the Army Ballistic Research Laboratory in Aberdeen, Maryland, and NASA's Ames Research Center. Why did he do it? Friends of Morris speculate that it was an intellectual challenge that got out of control. However, the jury found him guilty of intentionally accessing federal computers without authorization. Morris, was fined $10,000, and ordered to do 400 hours of community service work.

Life-threatening Viruses

While viruses that can shut down defense-related research computers are bad enough, experts have been greatly concerned about the possibility of the infection of battlefield computers which could disable these systems in the conduct of real armed conflict. Viruses can in fact be transmitted unknowingly by radio link in tactical field situations. One potentially vulnerable system of this type is the Maneuver Control System (MCS) used by commanders to plan and coordinate tank attacks and direct fire support during battle.

This concern, voiced in April, 1990, was another fear which became reality in short order when, just prior to Operation Desert Storm, several thousand Army PCs were found to have been infected with the so-called Jerusalem, Jerusalem-B and Stoned viruses. These apparently were introduced through the use of field computers for games such as Solitaire. This might have resulted in disaster had not virus detection measures been undertaken to clean up these systems. Desert Storm demonstrated for many of us just how seriously the computer virus issue must be taken—in time of war, viruses could threaten the effectiveness and survival of troops in the field.

Summary

The above discussion offers an overview of how we see the threat to information maintained in automated, computer-based systems in the 1990s. As with information security in general, the "threat" must be seen from a broader perspective.* Not only are we confronted by the traditional foreign intelligence services, but by international commercial interests and individual actors on the domestic scene who have their private agendas.

As a rule, classified files and databases are not supposed to be accessible even for legitimate reasons through conventional telephonic links, but this physical separation does not protect them from insider crime. And we are increasingly aware that much of the electronically stored information on which the defense and intelligence communities rely is sensitive but unclassified. These include data which if freely available might be used to undermine our technology lead in key areas such as high-speed computer processing, fiber optics, and manufacturing techniques. Consequently our concept of "the threat" in the 1990s and beyond must be broader than our former vision of foreign intelligence agents after classified government documents. And it must include, literally, the threat to the survival and integrity of the information itself in whatever form it is maintained.

What is an appropriate response to this multifaceted problem: on one hand, protecting vital information from interests who would use it against us, and on the other hand, ensuring that those who have a legitimate need for privileged information get it without trouble or delay? One answer, offered by Air Force Captain John McCumber in the following article, is to apply appropriate countermeasures where they fit. These include technology, policy, and security education, all of which, in the right combination, guard against the entire array of dangers. ■

* For a discussion of this new outlook, see "Future Threat" by Maynard C. Anderson in the August 1990 issue of the *Security Awareness Bulletin*.

A Study of Harassments and Provocations, February 1991

DCI Director of Central Intelligence

A new issue of *Harassments and Provocations* has recently been prepared by the DCI Security Form and issued by the Director of Central Intelligence for distribution within the intelligence and security community. As in previous editions under the same title, this booklet contains short case summaries of harassments and provocations against Americans assigned to or traveling in designated countries. These accounts, with general advice to U.S. citizens abroad, provide the security officer with excellent material for briefing personnel in advance of foreign travel.

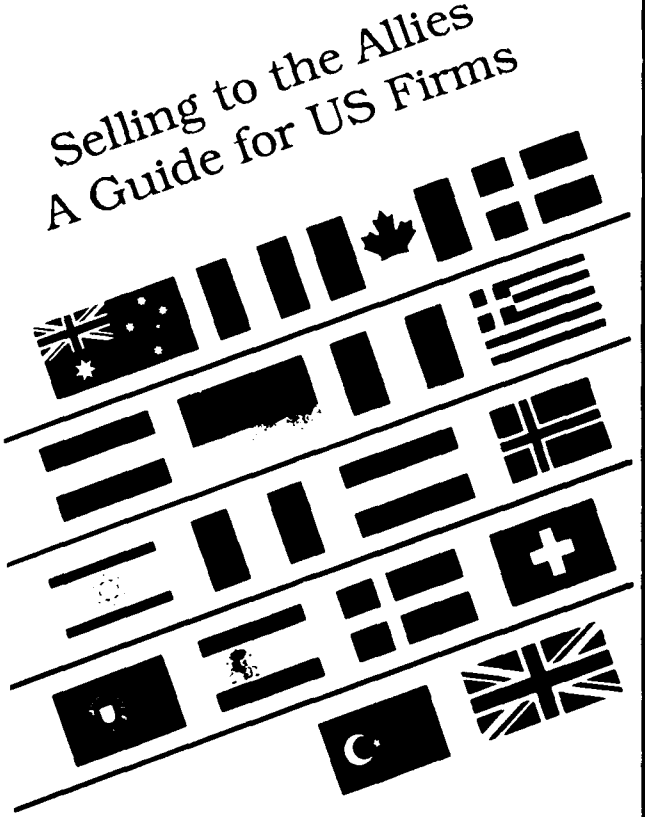
Since the publication contains national security information, it is classified as Confidential. Cleared defense contractors may request a copy from their regional DIS education and training specialist. Federal government security offices which have not received this publication by other channels may write to the Defense Security Institute, Attn: EPD, c/o DGSC, Richmond, VA 23297-5091.

Of Interest to U.S. Companies:

Selling To The Allies: A Guide For U.S. Firms is a publication to help U.S. companies that wish to do business with NATO and other allies with whom the United States has signed reciprocal procurement Memoranda of Understanding.

Part I provides general information that U.S. firms should know in order to export defense products and services successfully. Part II provides country-specific information.

Available through the Government Printing Office. Stock number 008-000-00557-5, cost is $7.50. Call (202) 783-3238 for ordering information.



Security Measures for the State-of-the-Art Workplace

by John R. McCumber

In the following article, Air Force Capt. John McCumber shows us how security measures for automated systems fit into the overall design for security management in the modern workplace. McCumber argues that although information is recorded or transmitted by differing media, it is, after all, information (and not the media) we are trying to protect. His system gives us a way to organize our thinking about the choice of policy and measures and a common-sense way to analyze problems as they arise. Computer and communication security are no longer isolated security activities that can be dealt with only by "technical experts." It is something that all security specialists and facility security officers must be able to deal with and understand.

Information Systems Security: A new perspective

In our rapidly changing workplace, computers routinely communicate with each other and electronic communication systems compute. Advances in technology have long since blurred the distinction between what we have been calling COMSEC (communications security) and COMPUSEC (computer security). *Information Systems* seems to be the most appropriate name for all the ways we handle data electronically. If nothing else, this name reinforces the idea that our emphasis is on the information and not on the technology used to act upon it.

What are the ways in which we handle data electronically and how do we provide the necessary security for that information? And secondly, how does this differ from non-automated security procedures.* The answers to these questions can be understood by someone who does not have a degree in electrical engineering or computer science. In fact, the same principles apply to the protection of information in both automated and non-automated systems. In this new age in which personal computers and modems are as commonplace as typewriters, and when even typewriters have memory chips, it is increasingly essential that the protection of electronically maintained information in the modern workplace not be the exclusive domain of a "specialist."

In addition, the range of information which we attempt to protect in automated environments often exceeds the narrow concern with safeguarding formally classified material. A new emphasis has been placed on the protection of information which may be sensitive, but unclassified. A recent congressional report stated that government and commercial databases "make information so readily available to foreign governments, competitors, and those having criminal intent, that uncontrolled access to them is a threat to national security."

Multi-Media Mystique

Information may take many forms and reside on any number of "media": printed documents, photographs, computer diskettes, magnetic tape—even the human mind is a storage medium. The many faces of information almost defy identification. The electronic technology used to transmit, store, and process much of this information has sometimes created a barrier to understanding as well. Over the last three decades, computer and telecommunications technology have revolutionized the way we handle information. It has also created an enviable subculture of experts and insiders. The "computer mystique" manifests itself in numerous ways. Most commonly seen is the weak grasp which management maintains on the systems development processes. Sensing a lack of technical insight, many executive officers have relinquished control over their information system resources.

Three states which information may take

Just as water (H_2O) can take the form of liquid, solid or vapor, so it is that at any given moment, information can exist in one of three conditions. At any point in time it is being either processed, transmitted or stored. The three states exist irrespective of the medium on which information resides. For example, you can store the same information on a computer fixed disk as well as on paper.

The distinction between the three states is fundamental to understanding the approach I have to offer for understanding (or evaluating) our security programs. For

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

A recent study has shown 75% of Federal agencies don't have a policy for the protection of information on PC-based information systems.

example, encryption can be used to protect information while it is transferred through a computer network and even while it is stored in magnetic media. However, the information must be available in plaintext (at least to the user) in order for the computer to perform the processing function. The processing function is another fundamental state which also requires specific security controls.

Three Critical Information Characteristics

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

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

SECURITY MEASURES

Up to this point we have looked at the nature of information in a number of ways: by considering first, three states in which it might exist: in processing, transmission, and storage. Secondly, the diverse media that can be employed to process, transmit, and store information. This would include everything from electronic media to paper documentation. And lastly, the three critical characteristics which information security systems must ensure: confidentiality, integrity and availability.

Now we are in a position to see how security mechanisms designed to protect information in automated systems fit into the total scheme of things. It is reasonable to assume that different security measures are appropriate for each state, for specific media, and for ensuring that each critical characteristic is maintained.

However, let's not get too complicated. For the present, I believe that it is adequate to organize our thinking simply around the proposition that in the automated world—as well as the non-automated world of hard-copy documents—security measures of specific types can be applied to the protection of information in the transmission, the storage and the processing mode.

But what types of measures are there? At the risk of sounding monotonous, again there are three, or more accurately, three layers of measures: (1) technology, (2) policy and practice, and (3) education and training. Altogether, they can be thought of as preventative devices and methods to prevent the loss, compromise, or destruction of information valuable to our national interest.*

At this point, we have a way of systematically evaluating the security posture of any information system whether it be automated or not. In the two-way table on page 9, we can map out the locations of available security measures which address specific vulnerabilities to information in each of three states. However, more needs to be said about each category or layer of security measures.

Technology

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

*As preventative mechanisms or methods, it might be more accurate, and consistent with contemporary parlance, to use the term "countermeasures." This term reminds us that one of the reasons security programs are designed is to counter or interdict the well-financed efforts of foreign intelligence services, and commercial organizations, to get at information which we hold in confidence.

Usually, organizations are built around specific tasks. The development of computer technology created the perception that a specialized group of employees was needed to accommodate the new machines which would process, store, and transmit much of our vital information. In other words, the organization was adapted to suit the evolving technology. Was this wrong? Not necessarily; however, it created the impression that technology exists for technology's sake. In reality, telecommunications and computer systems are simply among the many media on which information can be transmitted or processed.

Policy and Practice

Information systems security is not an off-the-shelf product which will be available at some future date. A security policy is simply the set of rules that determines whether a person can have access to a given category or piece of information. A recent study has shown 75% of Federal agencies don't have a policy for the protection of information on PC-based information systems. This would have to do with rules about user access control; physical storage requirements for media, software, and equipment; audit trails; and, of course, electronic transmission. Why is policy such a neglected security measure when it comes to automated systems? Do our security managers consider it to be too technical to deal with?

Because of an exaggerated reliance on technology, it's easy to think of security solutions as devices or add-on packages for existing information systems. Some security professionals are guilty of waiting for technology to solve that which is not solely a technological problem. And we are likewise guilty of pouring enormous resources into high-tech countermeasures as if they were the be-all and end-all of security for automated systems. Policy development must go beyond the hardware. Human beings use these products and devices and, as in any information security system, if we can't trust the people who have access, all other countermeasures are useless. Obviously, personnel security must be a strong element in the policy and practice layer.

In any event, any policy for protecting vital information resources must be backed by a set of standards which can and will be enforced by regulations that have some teeth. There must be established consequences which are applied when violations are discovered.

Education, Training, and Awareness

These first two layers, technology and policy/practice, represent the design and application of a security-enhanced information system. The last component of this dimension represents the *understanding* necessary to protect information. Although an integral aspect of the preceding two layers, education must be considered separately as it is capable of standing alone as a significant type of security measure.

Education, training, and awareness enhancement may be our most important security measures, for only by understanding the threats and vulnerabilities associated with our proliferating use of automated information systems can we begin to attempt to deal effectively with other control measures. The other side of the coin, of course, is knowing how to respond to the threat and how to neutralize vulnerabilities.

"...in any information security system, if we can't trust the people who have access, all other countermeasures are useless."

A LOOK AT THE WHOLE PICTURE

Now let's attempt to apply this framework for understanding or evaluating the entire security posture of one organizational unit. The chart on page 9 has several significant applications. But its initial, perhaps most important, value is that it helps us see the relationship between conventional security practices and measures, and those which belong to the automated information systems environment. In reality, they should be seen as belonging to one integrated system having both automated (electronic) and non-automated components. I have begun to fill in the open cells with security measures appropriate for each state of information. I do not suggest that this is an exhaustive listing of everything that is done to protect information in an automated environment, but this should give the reader an idea of how to implement the approach outlined in this article.

Looking for holes in the armor

As I suggested earlier, this framework can function as a checklist by locating available security measures or those already in place. By using this procedure as the foundation for a top-down approach to information systems security, one can begin to grasp the full scope of possible security measures. Even if there is no particular control available to counter a vulnerability, the knowledge that a vulnerability exists (and where) is a significant improvement over blind ignorance. In this case, the applied security measure would simply be one of awareness (one aspect of the third layer).

Take a look at your own information system. You may single out for scrutiny, systems information confidentiality during transmission and assess the adequacy of countermeasures in place. If you find this a weak area, you can then determine which security technologies help ensure confidentiality. Prescribe various cryptographic techniques and products to meet the need. Then repeat the process with other major types of technology which can satisfy security requirements for storage and processing. Having reviewed and possibly reinforced the first of three layers of countermeasures (technology), move on to policy and practice.

CONCLUSION

Recent outbreaks of information systems abuse, fraud, and actual espionage have shown that the threat is universal. Hackers, spies, embezzlers, and criminals are equal opportunity attackers—anyone with information is a potential target. Let's not exclude the unintentional vulnerabilities of natural disasters, errors and omissions, and ignorance. The widespread nature of the problem and the evolutionary nature of technology demand a strategy which can address the entire spectrum of information systems security. And, since the up-to-date workplace in government and industry includes automated and non-automated methods and media for handling information, no security officer should remain ignorant of the application of security measures which apply to automated systems.

A state-of-the-art security architecture is desirable for all individuals and organizations. That means, of course, an information system with the best and the latest technology, policy, and educational program available. And since the same principles apply to all information systems, there should be no arbitrary distinction between automated and non-automated information systems security when it comes to program responsibility.

Similarly, as recent technological breakthroughs continue to impact on the way we work in any setting, distinctions between the business community and government, or between military and civilian sectors seem equally inappropriate in terms of the application of security measures. Work-place automation has arrived--for everyone. From the Army outpost in Saudi Arabia to the crowded office in downtown Washington, security can be ensured by systematically addressing the whole process of protecting information—and not by partitioning off "computer security" as a an esoteric specialization. ■

Layers of Security Measures by Information States

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

New video at FilmComm

Jonathan Pollard—A Portrayal

Jonathan Pollard was an employee of the Navy, but because of his position as a counterintelligence analyst, he had access to hundreds of classified documents from the intelligence departments of many federal agencies—and at the time of his arrest, had stuffed enough of these documents in his apartment to fill a space 10' x 6' x 4'. Pollard is an American who spied for Israel. He is serving a life sentence for his espionage work. And the reason he is, is thanks in part to an observant co-worker who noticed suspicious activity and was smart enough to report it. This video reenacts the events at Naval Intelligence Command in Suitland, Maryland, that led to the realization Pollard was involved in more than just doing his job. Produced by the Defense Intelligence Agency, it runs for 18 minutes and is available in 1/2" or 3/4" videotape.

To order copies or for additional information write or call:

FilmComm
641 North Avenue
Glendale Heights, IL 60139
(708) 790-3300
fax: (708) 790-3325

PERMANENT COPY	RENTAL
$17.50 prepaid	$7.50 prepaid rental
$20.00 invoiced	$10.00 invoiced rental

The prices include all dubbing and handling charges except postage. Mode of transportation is your choice (UPS, First Class, Federal Express, etc.). The usual postage charge is about $2.50 except, of course, for overnight and priority shipping. Other security education videos available from FilmComm include The Dark Side of Espionage, Espionage Alert, and Espionage 2000. Please call them for additional products and information.

Computer Security Education

A computer security education package is also available through FilmComm—two texts with accompanying slides written and designed by Chris McDonald, an information systems management specialist at White Sands Missile Range in New Mexico. "Adventures of an Overseas Hacker" details Dr. Clifford Stoll's persevering detective work that uncovered the penetration attack against the Defense Data Network in 1986 and 1987. "Computer Viruses" is about just that—viruses. This presentation defines "virus," describes four viral case histories, and gives some potential virus defenses.

Permanent copy prices same as above; rental fee is slightly higher.

New AIS Requirements in the Defense Industrial Security Program

by Dennis Poindexter and Carole Jordan

Automated Information Systems (AIS) are ever-changing, but historically, the policy in the Industrial Security Manual (ISM) changes much less frequently. However, a new manual has been issued (January 1991) and some of the changes are significant. This article outlines the most significant changes (in the new Chapter 8) particularly for those who are already familiar with the "old" procedures. The previous edition of the ISM outlined AIS security requirements in Section XIII, having 21 pages. These requirements are now much easier to find due to the restructuring of the entire body of material into a 12-page chapter.

It is always easier to point out changes in the ISM than to actually implement them. For contractors with systems already approved, the approval process is simplified, and in certain situations, can be done by the facility. This was, in the past, the most common criticism of AIS procedures. Software controls are eased somewhat, and this was probably the second most criticized area under the former manual.

APPROVALS

In cases where the contractor already has several AISs approved, the approval process now requires only the submission of an Approval Request containing only a small part of the information formerly required by the previous ISM. Since there are usually some aspects of required safe; uards that tend to be overlooked when a contractor initially introduces an AIS, the Defense Investigative Service (DIS) anticipates many situations to arise, especially early in the implementation of this new process, when a traditional AIS Standard Practice Procedures (SPP) will also be required. Until the details of procedures are worked out, it is highly likely that both Approval Request and SPP will be jointly reviewed. The Approval Request has been reduced to the following as stated in Paragraph 8-105:

"a. Identity of the AIS to be used for classified processing: its physical location, mode of operation, the level of and special briefing requirements (if applicable) of classified information to be processed; and the lowest level personnel clearance held by any user on the system during classified processing.

b. List all equipment comprising the AIS, including the size and type of internal memory and other storage media. Indicate for each component whether classified information can be retained. Describe disconnect methods and switching devices for disabling equipments not to be used during classified processing periods. Include a block diagram of the hardware configuration that also shows any links to other components or AISs that are disconnected during classified processing.

c. Identify the types of operating system software and firmware used during classified processing. Specifically, name the operating system, the version number, and the Evaluated Products Listing (EPL)* rating or equivalent, if applicable. An AIS may be determined to provide protection equivalent to an identified EPL level as a result of documentary evidence that: (i) the AIS hardware is plug-compatible or object-code compatible with an AIS that appears on the EPL; or (ii) the AIS has been satisfactorily evaluated by the Cognizant Security Office (CSO) or by a CSO-approved organization as meeting DoD 5200.28-STD criteria or its equivalent.

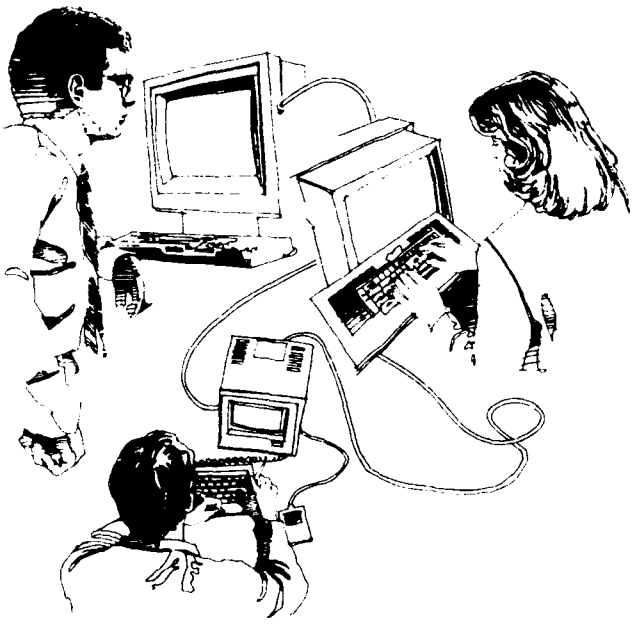
d. Describe the communication configurations and interfaces and identify all communications equipment and data transmission lines up to the point of encryption, which are employed by the AIS during classified processing. Include remote devices and protection procedures for transmitted data."

Some things were deleted and some added in the description of what is to ' e submitted. Deleted (from the previous ISM) were the following: (1) the use or purpose of the AIS, (2) the % of classified processing by level of classified material, (3) hours of operation, (4) the requirement to list all software used in conjunction with classified processing, and (5) the requirement to submit a special request for processing in the multilevel mode.

*EPL *The Evaluated Products List is maintained and published by the National Security Agency. It evaluates the technical protection capabilities of computer security products against well-defined published evaluation criteria. The List provides an authoritative evaluation of a system's relative suitability for use in processing sensitive information.*

Changes or additions related to the approval request are: (1) special briefing requirements for users, (2) lowest level of clearance held by any user on the system, (3) an indication for each component as to whether it can retain classified information, (4) identification of operating system software by name and Evaluated Products List (EPL) rating (applicable for modes other than dedicated), description of the security features/assurances and identification of data transmission lines to the point of encryption rather than to the point of disconnect.

The remainder of the information traditionally required for an AIS SPP must now be reflected in the facility SPP or a separate document. Only physical security, upgrading and downgrading, document accountability, audit trail records, and a contingency plan must be included in the Approval Request.



This approval process recognizes those contractors who have developed their AIS procedures to such a degree that "boilerplating" is common. Since they simply reuse the old SPP time after time, there is little necessity in reapproving the same words, over and over. For those contractors who have not standardized their AIS SPPs, the submissions of an Approval Request and the AIS SPP will be commonly required.

TRUSTED SYSTEMS

The most difficult areas come in the implementation of trusted computing concepts. This is a technical security issue, one most security officers may find a little uncomfortable until the terminology becomes more familiar. There is more to this than just reading the ISM. It requires close coordination with the facility Management Information Systems/AIS staff.

The use of trusted systems is apparent throughout the new re-write. Levels of trust come from the security requirements in DoD 5200.28-STD. This document is an evaluation standard used by the National Security Agency (NSA) in rating products that appear on the EPL. From most, to least secure, they are A1, B3, B2, B1, C2, C1, D. Each level has specified mechanisms which would be implemented to qualify for the rating. The level required depends on the mode of operation. The ISM allows "an equivalent" implementation so a contractor may use trusted products from the EPL or demonstrate that it has the mechanisms of the level incorporated in the system.

The EPL, along with several other pertinent references, are part of the NSA Products and Services Catalogue, available by subscription from the Government Printing Office. At the same time, it might be wise to obtain DoD 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria", and CSC-STD-003-85, "Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments." These provide technical guidance to systems developers on security requirements, useful if the facility does not have EPL rated systems and must demonstrate the security features and assurances for DIS approval. For systems not operated in the dedicated mode, trusted software, or an "equivalent" is required.

SELF APPROVAL

A new paragraph has been added for contractor approvals. Contractors may, at DIS discretion, be designated to approve their own systems. This has been done for some time in several DIS regions, on a test basis. This would require technical expertise available in some facilities, and management support for compliance with the procedures. Approvals are limited. First, systems must be in the dedicated mode. Second, similar systems must have already been approved by the CSO. Third, the processing level can be no higher than the CSO-approved systems.

Electronic typewriters, basic function calculators, and test equipment having volatile memory and no other storage media such as magnetic disks, do not require advance approval. Security requirements for these types of equipment are now required in the facility SPP.

GENERAL REQUIREMENTS

The new Section 3 in Chapter 8 combines the remainder of the requirements in a logical flow and contains requirements for the SPP, mentioned above. It also

renames the Systems Security Officer as the Information Systems Security Officer (ISSO), which is consistent with other DoD use of the title.

This section authorizes (with DIS approval) two technical additions: (1) use of data reduction programs in auditing, where "there are extremely large volumes of audit data in electronic form" and (2) procedures to place an account in a dormant status or otherwise deny access to a user who no longer requires use of the system, pending recovery of the information in the user account.

Software controls are the most significant change in Section 3. Paragraph 8-309 covers the protection of software and data. Paragraph 8-309a states that: "Software and modifications thereto shall be developed by contractor personnel who are appropriately cleared." This requirement is being reviewed and could be changed in the future so that only system and security relevant software need be developed by cleared people. Paragraphs 8-309a and 8-309b continue:

"If the software contains security related functions (*e.g.*, declassification, access control, auditing), it must be validated to confirm that every security related feature is fully functional before it can be used during a classified processing period.

b. **Unprotected software.** Other software may be introduced into a classified processing period only from a source which is write protected. Software used during classified processing periods, without write protection, must be classified and safeguarded at the highest level of information processed."

The write protection requirement affects PCs with hard disks, where most of the software resides. Unclassified media will have to be write protected, or it must be safeguarded and classified after being used during a period of classified processing. The software that does this will be security related, assuming it is done with software and not a hardware switch on the write head wire.

Software disconnects will be authorized only where a system meets at least the B1 level of trust, and will still not be authorized for Top Secret. This will impact on some dedicated mode systems already using software disconnects.

The paragraphs on clearing and declassification of storage media (8-313 and 8-314) contain two important changes. First, nearly all procedures for declassification and clearing will be provided by the CSO, including overwrite guidance on the declassification of non-volatile memory and rigid storage media.

Second, there is a new requirement for declassification software to "be developed and tested prior to the time storage media or memory needing the software is declassified. The software must be safeguarded, prior to and following its validation, at the highest classification level in which it will be used to declassify an item." The requirement for protection (as system software) is not new, but validation of it is.

MODES AND LEVELS OF TRUST

There will be four modes: dedicated, system high, partitioned, and multilevel. The addition of partitioned mode is not new to the Department of Defense, but it is to industrial security. Dedicated mode remains the same; *i.e.*, all users have a Personnel Security Clearance (PCL) and a need-to-know for all information in the system. In system high, all users have a PCL and receive special briefings (*i.e.*, formal access approval) for the highest level of classified information, but some do not have a need-to-know for all of it. Partitioned mode is slightly different, in that all users have a PCL for the highest level, but not necessarily special briefings and need-to-know. Multilevel is not changed; users need not have a PCL for the highest level processed in the system. Multilevel is restricted to two adjacent PCL levels, such as Confidential and Secret, or Secret and Top Secret.

The addition of special briefing requirements will have some impact in systems which are now system high. Levels are the levels of classified information (Top Secret, Secret, and Confidential). Special briefings are required for material for which access is restricted, such as NATO, COMSEC, CNWDI, and special access material. In the past, if some users did not have a need-to-know for this material, they did not receive briefings and the approval could be made as system high. Now it will be partitioned, which requires a higher level of computer-based security (at least B1). This is reflected in a "level of trust" provided by the system. The level of trust required depends on the mode of operation.

Level of Trust Required	
Mode of Operation	**Minimum level of trust**
Dedicated:	Not required
System High:	C2
Partitioned:	B1
Partitioned with more than two categories:	B2
Multilevel:	B1
Multilevel with Top Secret:	B2

Audit trails are dependent on the mode and level of trust to be provided. As specified in Paragraph 8-305, all systems require three types of records and logs:

"(1) Maintenance and repair of hardware, including addition or removal of equipment or devices to the unit.

(2) Initiation and termination of significant system security-related events (for example, disconnecting and reconnecting remote terminals/devices, upgrading and downgrading actions, and application/reapplication of seals to equipment/device covers).

(3) Description of the classified hardcopy output produced during each classified session."

The last is a new requirement, though often previously done. The description of the output must contain a short title, the level of classification, and the number of copies created. Dedicated mode requires additional audit trails on "the identity and time of access by each person having access to the AIS." All other modes must comply with the auditable features required of the level of trust as described in DoD 5200.28-STD.

NETWORKS

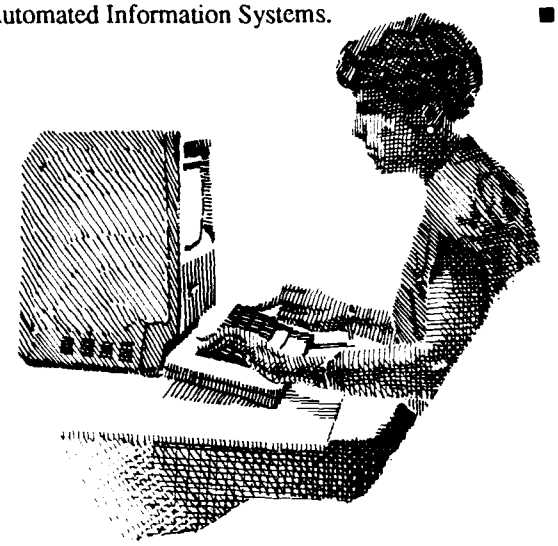
This is an entirely new section, recognizing the importance of networks. Networks are classed as two types, interconnections of approved AISs and unified, where the net is considered as a whole. Paragraph 8-401a states:

"When approved AISs are interfaced or networked between a contractor and a User Agency, between cleared facilities of one contractor, or between contractors, the entire system must be approved as a network. The DIS has been designated to approve AIS networks when only cleared contractor facilities are involved as part of the network. If more than one CSO is involved, appropriate DIS management officials will determine which CSO will serve as the single approval authority for the network. The designated CSO will determine the restrictions and limitations that may be applicable. When the network involves a User Agency activity, then the DIS Deputy Director (Industrial Security), or his designee, and the Designated Approval Authority for the User Agency involved will work out suitable network security arrangements under the terms of a memorandum of agreement negotiated between the government parties." (Since the requirement for a memorandum of agreement is new, an article is being prepared for publication in the Industrial Security Letter on this subject.)

This recognizes that networking may change the mode, thus requiring additional security, and that interconnection may have an impact on the levels and categories authorized to be received by a particular node. It also, for the first time, involves the User Agencies in the approval of systems being connected to their nets. Although the ISM does not require it, a facility may need to designate a network security manager as a focal point for security issues.

CONCLUSION

Overall, the procedures are easier to read and understand. That doesn't mean there won't be debate, but it does mean the debate will be narrowed, hopefully to issues that concern how classified information can be better protected in Automated Information Systems. ■



About the authors: Dennis Poindexter is the former chief of the AIS Security Division, Industrial Security Department of the DoD Security Institute. He recently joined the Internal Revenue Service as a senior analyst. Carole Jordan is senior computer security specialist at Defense Investigative Service headquarters. She was formerly with the National Computer Security Center, NSA.

Stop Computer Viruses in Your Tracks

by Jim LeVangie
Computer Systems Center, Arlington, Virginia

The following article is reprinted by permission of the Joint Industry/Government Security Awareness Group (JIGSAG), Washington, D.C. This group, comprised of security officers from industry and the Department of Defense, meets regularly to create or identify security education materials. This article on viruses is just one of their products. Although examples of viruses and anti-virus software packages apply to the Macintosh environment only, much of the discussion is relevant to IBM and IBM-compatible systems. Mr. LeVangie is a member of JIGSAG.

Nothing is more frustrating to data handling than being subjected to a "virus." A virus is a program, usually hidden within data or other programs, which attaches itself to other applications or files. Its function is to "infect" other programs with copies of itself. Therefore, it can clone itself, multiplying and seeking new host systems. The virus programs, like infectious microorganisms, are often small, consisting of only a few lines of programming code which are easily hidden in "healthy" software. Initially, exposure to such insidious programming was thought to take place only if programs from questionable sources or bulletin boards were used. Members of the JIGSAG Committee, however, have been exposed to "viruses" in systems using restricted programs obtained directly from a reputable company.

Why me?

Why are viruses appearing now? (Or more accurately, since about 1987 in Europe and 1988 in America.) The simple answer is progress. When the U.S. Navy was cleaning moths out of tube computers and placing the bodies in the work log—the origin of "debugging" the computer—control software was kept in a separate part of the memory banks. To reprogram the computer it was necessary to remove the read/write cable from the data memory banks and plug it into the control memory banks. But then came our solid state circuits and microchips. Access time and convenience now place data and control instructions into the same memory with only an ID or locator to separate control from data.

The spread of infectious computer virus programming could easily have happened accidentally. But it didn't! "Trojan horses" were intentionally placed in the Space Physics Analysis Network computer (SPAN—an international computer network) by the now infamous German Chaos Computer Club, known for using operating system errors to access computers of institutions like the German Research and Experimentation Institute for Aviation and Acronautics, the European Space Authority, NASA, and SPAN.

What can the virus do to my system?

Viruses may be benign or non-malicious, in which case they replicate themselves, displaying messages on the screens, beep, or do other innocuous things. An example is the virus that appeared in the Apple Systems on March 2, 1988. This Universal Message of Peace or "Peace" virus only produced a message.

Viruses are also malignant or malicious, making changes to host system data and applications. Following the Peace virus, Apple Systems soon experienced a "Scores" virus, then various strains of the "Nvir" virus (which will be explained later). The virus as a technological phenomenon has already infected enough programs and networks to make major computing disasters inevitable in the foreseeable future.

Help!

Enough of background and history. Let's pull together some information that can help you now. We'll tell you of examples and results of virus infection and give you some idea of when or if you might be exposed to such viruses. Also below is a quick list of virus utilities and an explanation of their capabilities.

The best method for stopping a virus is to delete the infected file and replace it with one that is known to be healthy. However, in cases where no clean backup copy is available, this list of utilities may help.

Easy Prevention

Be sure your copy of a utility program has the write protect in the protect position. A recent installation of Disinfectant was stopped by the SAM, which had been already installed, with the alert that the Disinfectant disk was being attacked by an Nvir virus at installation.

Anti-Virus Utilities Currently Available for Macintosh Systems

AGAR Provides detection by offering itself as a sacrificial medium for the attacking virus. It, therefore, requires periodic checking of ResEdit to see if drive resources have changed.

AntiPan Automatic reaction. The AntiPan utility searches for Nvir and Hpat (an Nvir clone) infection and attempts to eradicate them when found. Damage to system varies with extent of infection and type virus.

AntiVirus Automatic reaction. This utility searches the system files and applications for Nvir infection. When a virus is found, it attempts to eradicate them leaving an "immune system" behind to prevent further infections from Nvir.

Blood Test Detects by scanning for INIT, DATA and Nvir resources. Initiated by the operator, this utility searches for the above identified virus resources in system files and applications. An option to search for patched traps is also available.

DisInfectant Automatic reaction. This utility reportedly recognizes Nvir, INIT-29, ANTI, MacMag, WDEF, ZUC, MDEF, Frankie, and CDEF viruses along with all the known variations and clones. It does not recognize the Dukakis virus which propagates between HyperCard stacks and is very rare. Equipped with a startup document (INIT) which protects against infection, and a repair application which can be initiated for automatic healing/repair of an infected system.

Ferret Automatic reaction. This utility searches files for signs of the Scores virus. The infected fields are identified and flagged for options of: delete, repair or ignore.

Fever Provides a detection capability only. Unlike AGAR, Fever has an automatic notification if an infection has occurred.

Gatekeeper As it sounds, this utility is a control panel device which allows you to specify in each application file on the hard disk, whether the file resources or data fork can be modified. Three different types of modifications are available and can be independently allowed or prevented.

Modifications can be controlled that are performed by:
1 - the application itself
2 - the system file, or
3 - by other files.
No repair feature is available since it is expected you will stop the virus before entry.

Interferon Automatic Reaction. This utility searches files for signs of Scores, Nvir, and Sneak viruses. If found, an option of deleting files from disks or drives is provided.

KillScores Fully automatic reaction. The utility searches all files on a disk for Score virus infection, and attempts to repair them.

N.O.M.A.D Fully automatic reaction. The NOMAD utility searches disks for the Nvir virus and removes Nvir resources when found.

Nvir Assisin Fully Automatic Reaction. The Nvir utility searches disks for the Nvir virus, removing it if found.

Repair Repair capability only. The repair utility removes Nvir virus infection from an application file, however, another utility must be used to first identify the infected file.

RWatcher Automatic blocker for programmers. The RWatcher utility is equipped with a startup document (INIT) which protects against infection. It watches for certain resource modifications to be attempted, then stops them. It looks for the most common Scores and Nvir modifications. However, using the ResEdit, other known, and unwanted, resource modifications can be tracked.

SAM Automatic blocker that scans new disks when installed. SAM is short for Symantec AntiVirus for the Macintosh package. This utility is a control panel device which allows you to specify in each application file on the hard disk, whether the file resources or data fork can be modified, thus providing a detection and prevention capability known as the SAM Intercept initialization program. The SAM Virus Clinic is an application that checks for and eliminates existing virus infections. The SAM Inter-

cept initialization program has various levels of thoroughness in monitoring changes. It provides immediate search of disks being installed plus watches for ten different file modifications performed by currently known viruses, not all common at this time.

Symantec Utilities Guardian and Shield init

Automatic blocker. This utility may provide some type of virus protection. However, the only type of attack prevented appears to be against disk directories. The Macintosh Encyclopedia has found no such an attack by currently known viruses.

Vaccine Automatic blocker. The Vaccine was the first antivirus utility designed for Macintosh systems. The Vaccine utility is equipped with a startup document (INIT) which protects against infection by screening certain suspected modifications to system resources. If found, Vaccine alerts the operator to the modification and asks permission to let the modification occur. As in other initialization programs, no repair capability is provided.

Virus Detective Automatic blocker and scans new disks when installed. This utility is a DA which searches drives for files infected with Nvir, Hpat, Score or INIT 29 viruses. When found, the files are flagged and options of "repair" or "delete the file" are presented.

VirusRx Scan only. This utility scans disks, then presents a list of files that may be infected. Since it only looks for possible irregularities, the false alarm rate is high and another utility should be used as proof positive. Again, as with other scan utilities, repair features are not available.

For IBM Compatible Systems

Anti-Virus From Central Point Software

ViruSafe From EliaSham Software, (407) 682-1587

Listing of privately-produced materials does not imply an endorsement by the Department of Defense.

There are currently three techniques for approaching the virus problem.

- Block the virus by scanning for known virus modifications and utilities. This technique may or may not check the disk upon first entering into your system. To make the utility more user friendly, the utility should have an alert-flag or notice when a suspected virus is found.

- Some utilities simply check existing files to see if they are infected. This type usually produces a list of the results of the inspection. It may or may not have a blocker to prevent further infection.

- Some utilities have the ability to disinfect the files. It depends upon the virus and disinfectant technique as to the extent of damage done to the data.

Remember, write protect all virus utility disks before placing them into a computer system that has not been checked. In addition, some utilities may not completely remember all the viruses, allowing sleepers to reappear. It is good practice to periodically run a virus check on your system even if you have not entered outside data or programs recently. Better to be safe than sorry.

So what's a "Trojan Horse"?

The term is used to describe a destructive program that has been disguised as an innocent one. In the SPAN case mentioned above, the program allowed the hackers to enter previously visited systems more easily each time. The Trojan Horse programs were around long before viruses became a serious problem. They are infamous for using attractive fronts such as a games or graphics (especially pornographic games found on bulletin boards to keep the victim's attention while the program does it's damage).

The history of the Trojan Horse in the business world includes more subtle procedures for embezzlement or industrial espionage. Some, programmed for self-destruction, leave no evidence behind except for the damage caused. In banking, a technique known as "salami slicing" uses the "horse" to slice off small sums or accounts, unlikely to be immediately noticed, and transfer them to the account of the thief.

Beware of inserting any new or healthy disk into a questionable computer file. Be sure your copy of any utility has the "write protect" in the "protect" position. (The little tab on the left trailing edge of the disk or the square tab on the edge of a floppy.) An easy way to

remember: If you can't see through the hole (or see the disk in the case of floppies), don't put it into a questionable system! This applies especially to anti-virus utilities you expect will protect your systems now and in the near future. As in new utilities, it is always good practice to copy the original disk for storage and work from the copy. Again, be careful to write protect your working copy.

Current virus utilities use three techniques to fight viruses.

1. *Blocking the virus by scanning for known virus modifications and utilities.* This technique may or may not check disks upon first entering into your system. To make the utility more user friendly, the utility should have an alert flag, or notice, when a suspected virus is found;

2. *Scanning or checking existing files to see if they are infected.* This type of utility usually produces a list of the results of the inspection;

3. *Disinfecting or removing the virus program from the files.* Remember, it depends upon the virus and disinfectant technique as to the extent of damage or reconstruction of data results. Some utilities do have the capability to perform two or more of the above techniques automatically or upon initiation.

Anti-Virus Practices

As with dependency upon any system, the establishment of routine practices will markedly reduce your possibility of infection. It only takes a few minutes each week to protect your computers against the current known virus situation. Such practices include:

- Installing a blocker type utility which can save you much grief. If you have a number of people working on the system, be sure to check your utility periodically to ensure it is still installed.

- Acquire software with care. When purchasing software, be sure the source is reputable and the software is in a factory-sealed container. Remember, the virus propagates most effectively from unlicensed, borrowed, public domain shareware/freeware, or personal software. But even commercially purchased software can have viruses. Therefore, the best policy is to check everything with an effective anti-viral program/utility.

- Lock all your original software upon receipt. Make and use copies only. Never unlock your original file copy. But remember, check the original for viruses before locking and relying upon it as a source.

- Plan for emergencies by making periodic backups of your hard drive, too. Once a week is recommended.

- Before and after making your backups, use a virus search utility to ensure your fall back position is healthy or clean. Once confirmed, then lock it!

- Before using the new disks of software or data, ensure your blocker or scanner utility is applied. Some blockers automatically check disks upon every installation.

- The bottom line is to control all inputs. If you leave your system hooked to an active telephone modem, always pre-screen any data or programs entered into your primary computer system. Always suspect any software or data no matter what the source.

- Educate all users of your systems to viruses and how to protect against them. Ensure all are familiar with the virus utilities available to your system and establish routine procedures similar to those listed above.

Indications of a Computer Virus

The following is a list of indications that a virus infection has taken place.

This is not a complete list nor will it be a certainty that you have acquired a virus if the indication is present. Many viruses give no sign of their presence until after the damage is done.

1. PC is sluggish and saving the working data does not appear to speed up operations. (Note, extensive data in rapid access/temporary memories will sometimes slow down computer operations.)

2. New filenames appear with no users admitting to ownership.

3. Files become corrupted, showing incomplete data, difficulty in printing or errors, etc.

4 Unexpected messages appear. Messages may be completely foreign or appear to be default messages generated by the computer (*e.g.*, "Peace to the World" versus "Command key not available at this time.").

5. New data appear in stored files. Also, your PC does not retain the proper data even if left on after updating.

6. Files grow in size. Infamous to the Nvir, this problem will cause problems with your computers parity

check causing alerts or computer bombing. If allowed to continue, system restart may be prevented.

7. Files disappear or are lost without reason. This problem can really start you wondering about your sanity. You may not be as dumb as you think you are; check for a virus!

8. Disk indicates unusable. Ever taken a disk full of information you have just generated, inserted it into your PC and received an alert: "Disk unreadable!", "Disk improperly formatted", or "The disk 'AAAAAAA' needs minor repairs. Do you want to repair it?" Don't give up, check for a virus!

A Couple of Viruses You Might Meet

Viruses vary according to the computer system that they target. The viruses can be identified by the area of the system they infect or the type of mechanism they use for replication. With this seemingly unlimited field, we have selected the most common system involved with desktop publishing, and the system most commonly used for inter-company communication and cooperation among our members: the Macintosh system. We found another problem in pinning down the classification or strain of virus created by hackers. It is easier to modify an existing virus than to develop one from scratch. Many viruses are apparently being modified numerous times with different end functions and effects on systems. The following list is, therefore, an attempt to identify the most common and referenced viruses on Macintosh systems.

Nvir Virus

This is one of the first widespread viruses detected and identified, in Europe in 1987 and the United States in 1988. Macintosh files are made of two parts: the Data Fork and the Resource fork. The Data Fork contains traditional data such as text, numbers, formatting commands, etc. The Resource Fork holds Macintosh resources or programming elements, usually in octal format. Each resource is identified by its type (four-letter code), an ID Number, and in some cases a name. One of the viral resources added to files infected with Nvir Virus was identified as resource type "Nvir"—the source of the Nvir virus name.

NVIR occupies both memory and disk space which by its existence can cause problems. It infects the System File but not Note Pad or Scrapbook files. It doesn't appear to create invisible files (files whose icons do not appear in the Finder, and whose names do not appear on scrolling file listings.) There is no delay with Nvir. It begins spreading to other applications immediately upon running the new infected application. The finder and DA Handler usually become infected as well; however, with the later strains of NVIR A and Nvir B, document files do not appear infected or modified.

An early version of Nvir was apparently malicious, for it reportedly destroyed files in the System Folder; however, there have been few reports recently and this strain may now be extinct. Two basic strains of the Nvir are known to have been developed (and identified by John Norstad and his international group of Macintosh programmers, enthusiasts, and virus experts). These strains have been identified as Nvir A and Nvir B. Nvir A and B only reproduce initially; however, there is evidence that a counter is started, and counts down whenever the system is turned on or an infected program is started.

Nvir A after countdown will sometimes say (if MacinTalk is installed) "Don't panic", or just beep. It normally occurs at system startup or when an infected application is run. The alert may be repeated.

Nvir B after countdown will beep. No MacinTalk equivalent in comment has been found. It normally occurs at system startup or when an infected application is run, and may beep twice.

Good Grief! Nvir A and B—The two basic strains have been found to mate and reproduce themselves resulting in parts of their parents or in other strain procedures and effects to appear.

Nvir B Clones—A number of Nvir B clones have appeared which are identical to Nvir B with a few very minor technical differences.

Scores Virus

First discovered in early 1988, the Scores Virus was named after the invisible "Scores" file that it creates in the infected systems. Scores occupies both memory and disk space; however, it does not infect or modify document files, only applications and system files. Scores infects System, Note Pad, and Scrapbook system files. It also creates two invisible files in the System Folder named "scores" and "desktop" (not to be confused with Finder's Desktop file.) Two days after system infection, the Scores virus program begins to spread to each application being run. The Finder and DA Handler will usually become infected also. Scores is not itself a malicious/malignant program; however, by occupying memory and disk space, it can cause problems. Problems with MacDraw, Excel, system crashes, and so forth, have been reported as a result of errors in Scores programming. Of particular note is a problem with Apple System Software release 6.0.4 and later. Similar resources with the same type and ID as Scores causes loss of the Apple Software when cleared of

Note Pad File Scrapbook File
Normal Healthy MacIntosh

Note Pad File Scrapbook File
MacIntosh Infected with Scores

the virus. Reinstallation of the software will be necessary.

There is sometimes an easy way to spot a Scores virus. Open your System Folder with View by ICON. Note Pad and Scrapbook files should look like little Macintoshes. If they look instead like blank pages with turned-down corners, your software may have been infected by Scores and still have normal Note Pad and Scrapbook icons. Another way to check is to use ResEdit Utility to find the Score's hidden desktop file inside the System folder. The Scores' Desktop file has an extra space character at the end of its name.

Other names from the Scores Virus

ERIC Virus
Vult Virus
NASA Virus
San Jose Flu Virus

There are a lot of good references on computer viruses. Some are listed below. It's to your advantage to know at least something about them—to recognize when you've got one and the damage it can do. Security awareness is our best hope for keeping our data and systems secure.

Resources:

1. *Encyclopedia MACINTOSH* by Craig Danuloff and Deke McClelland of SYBEX Inc., 2021 Challenger Drive #100, Alameda, CA 94501
2. *Computer Viruses A High-Tech Disease* by Ralf Burger of Abacus, 5370 52nd Street, SE, Grand Rapids, MI 49512.
3. *Computer Viruses, Worms, Data Diddlers, Killer Programs, and Other Threats To Your System: What They Are, How They Work, and How To Defend Your PC, MAC, or MAINFRAME*, by John McAfee and Colin Haynes Re: St. Martin's Press, 175 Fifth Avenue, New York, NY 10010.
4. *Computer Virus Guidelines for PC Users and Managers*, a quick-reference security guide from Dr. Rodger Quene, ISG.
5. Various internal help information from the associated utilities and programs being addressed. Such inputs include:
   a. SAM Intercept Help
   b. *Disinfectant Manual* by John Norstad of Academic Computing and Network Services, Northwestern University, 2129 Sheridan Road, Evanston, Illinois 60208.
   c. *How To Use Virus Rx* by Apple Compuer Inc.

COMPUTER SECURITY A TO Z

The risk of loss, damage, or compromise of classified and/or sensitive information is increased by not following good computer security practices. Each person is responsible for ensuring the security of his/her computer equipment and software. Following are some security awareness reminders from A-Z to help you practice good computer security. (Extracted from News Bulletin, March 1991, HQ US Army, Europe and Seventh Army)

Authorized software only is to be used. This is software that has been procured through approved channels.

Beware of strangers bearing gifts of software.

Classify floppy disks at the highest level of information processed by the systems.

Disposal of floppy disks no longer needed or usable must be done in a secure manner.

Emanations from computer terminals must be contained by zoning, shielding the work area, or using approved equipment.

Floppy disks should always be handled carefully and stored according to their classification label.

Good computer security practices include logging off your computer when not in use or when leaving your office.

Hard disks should be protected using all available means, such as approved password systems and key locks.

Inform your Security Office of all suspected computer security incidents.

Just say no, when asked for your password.

Keys to terminal must be kept in lockable containers when not in use.

Labels must be placed on computer output and magnetic media to identify classification levels.

Maintenance of classified computer equipment must be performed by cleared individuals or in the presence of a technically-qualified cleared escort.

Need-to-know principle applies to computer access, not just to classified information.

Odd or unofficial requests for computer information such as surveys should be reported to your supervisor or security officer.

Practice good digital hygiene; don't exchange programs.

Questions regarding computer security can be addressed to your security officer.

Risky behavior, such as using unauthorized modems or playing computer games, can lead to a virus and is strictly prohibited.

Secrets in the computer require the same protection as secrets on paper.

Tear off printer output immediately, and tend to it appropriately.

Users are the key to effective security.

Viruses in our computers can be avoided by using only authorized software.

Watch for suspicious changes to files in personal computers (PC) operating systems. The changes may have been the result of a computer security problem such as a virus.

X-pired accounts are a security hazard; have yours removed from the system when no longer needed.

You are responsible for the security of your computer resources.

Zero tolerance for violating computer policies and practices.

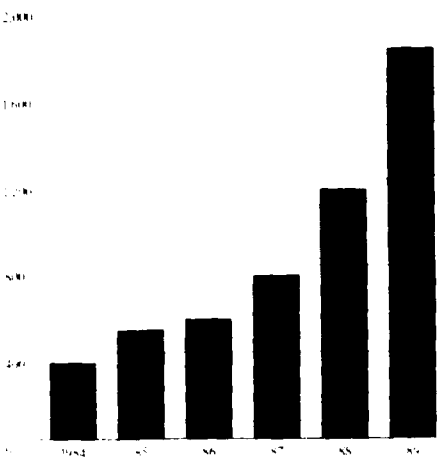
Security Awareness . . . The Threat Is Real

Soviet Intelligence Targeting of the US Scientific Community, a report published in August 1990, is available from our Educational Programs Department. Written by intelligence community analysts, this is a basic tutorial for those in contact with the Soviet scientific community. It describes how the Soviet intelligence services exploit contacts between U.S. and Soviet scientists.

The document focuses on the USSR's efforts to use scientists associated with the Soviet Academy of Sciences to collect U.S. scientific-technical information. Soviet scientists often have been tasked to collect biographic and assessment data on U.S. scientists and aid in evaluating Western scientists' personal vulnerabilities and receptivity to recruitment.

To order a copy, please see the publications listing on the next to the last page of this *Bulletin.*

Figure 1
Soviet Scientists Requesting Visas To Visit the United States, 1984-89



SECURITY *Awareness* in the 90s

Proceedings of a symposium co-hosted by the Defense Personnel Security Research and Education Center and the Department of Defense Security Institute, December 12-14, 1990, Monterey, California. This 257-page record of the recent Monterey symposium is especially valuable to security professionals in government and industry whose primary responsibility is security education and awareness enhancement. The Monterey symposium brought together both higher level policy-makers and experts in a number of fields who shared with us their skills and strategies for reaching and influencing wide-spread audiences. Among the presentations included in this volume are the following:

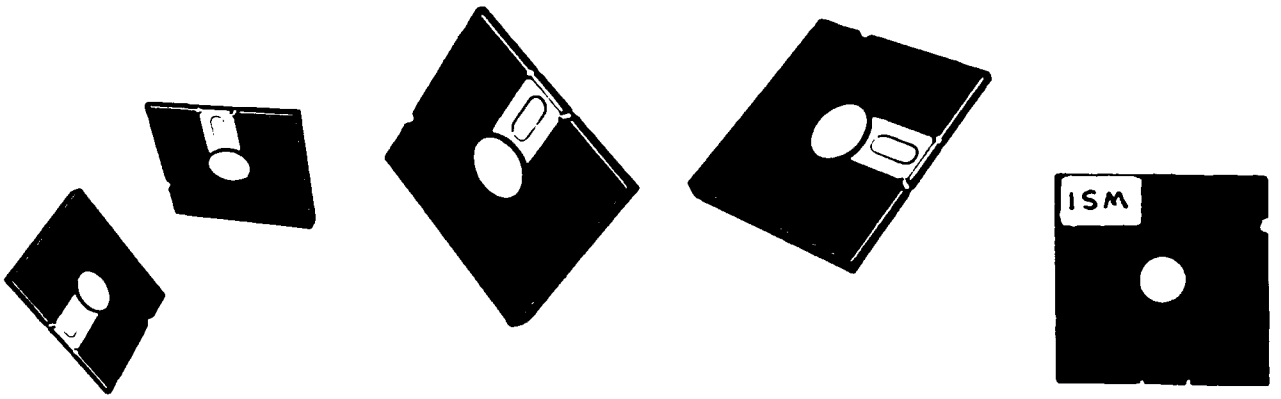
- ***Geopolitical Trends***
- ***Public Opinion***
- ***Advertising***
- ***Training Technology***
- ***Program Evaluation***
- ***Strategic Planning***
- ***Planning for the Future***

We have a limited number of copies of these proceedings remaining in stock and we want to make sure that they are available to security professionals who would make the best use of them. To request a copy please write us at the DoD Security Institute, Attn: EPD, c/o DGSC, Richmond, VA 23297-5091 or call us at Autovon 695-4223 or Commercial (804) 275-4223.

The New Industrial Security Manual On Computer Diskettes

Since the issuance of the new January 1991 *Industrial Security Manual*, several private sources have come out with the manual on computer diskette and are marketing this product in various formats. Obviously, PCs have now made it easier for FSOs and other security professionals to quickly search and retrieve information and relevant text from electronically stored files. And it is clear that in the near future, the standard way for referencing lengthy government regulations, manuals, and reports will be by key-word search and retrieval by electronic methods.

What follows is a listing of ISM packages for computer application that we presently know about. We would be more than happy to make our readership aware of any others that come to our notice in subsequent issues of the *Bulletin*, but no official endorsement of any product should be inferred from this listing. One word of caution: Due to the possibility of omissions and errors in electronically stored text files of the ISM provided by private vendors, these should not by themselves be cited as "authoritative" when making decisions about contractor obligations under the Defense Industrial Security Program.



- **The ISM on Diskette**. Includes the full text of the 1991 ISM in ASCII format with an index (not found in the official hard-copy ISM), LIST—a search and retrieval software package, and a users guide. This product is distributed in four 5.25 inch diskettes for IBM compatible systems by FilmComm, 641 North Avenue, Glendale Heights, IL 60139. Phone (708) 790-3300. The price of $17.50 includes all charges except postage. The first class postage charge is about $2.50. UPS and Federal Express are also available.

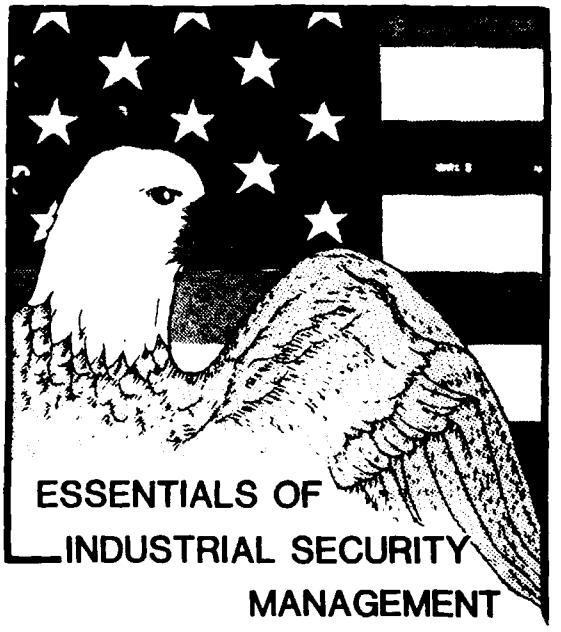
- **Automated SPPs and ISM**. Diskettes for either IBM compatible or Apple Macintosh systems are available from the National Security Institute, 161 Worcester Road, Framingham, MA 01701. Phone (508) 872-8001. According to NSI, this is a complete on-line PC-based security library of current ISM requirements and company security procedures you can custom tailor to fit your facility's security program. The package is designed for use with Microsoft Word or Word Perfect word-processing packages and is available in 3.5 inch or 5.25 inch diskettes for $495.

- **SIMS On-Line ISM**. Includes the entire 1991 ISM with the latest issues of the *Industrial Security Letter* also on magnetic media. The *ISL*, issued by the Defense Investigative Service, is an authoritative vehicle for guidance on ISM requirements. Included with these text files is a users guide and *Golden Retriever*, a versatile search and retrieval package which can be used to process other text files. Both IBM compatible and Macintosh versions are available. The entire package sells for $495 and can be purchased from Sims Software, Box 607, Solana Beach CA 92075. Phone Tom Fleming at (619) 481-9292.

DoDSI Correspondence Course Update

REVISED *EISM* AVAILABLE

The updated *Essentials of Industrial Security Management*, DS 2103, is available for enrollment. The new edition has been thoroughly revised to reflect the policies and procedures in the January 1991 *Industrial Security Manual (ISM)*.



Besides aligning its content with the new *ISM*, we gave the new *EISM* a facelift. Its format boasts shaded headers for captions, chapter-specific running heads, and handsome flowcharts and topical charts. Of course, we've kept the Electric Widget Company and Electric Widget Services, and you'll still find Harriet Hornesby, Milo Mertz, Wanda Fishtank, Avery Ivory, Jimbo Duggins, and the rest of the gang. You'll still find completed samples of personnel security forms and a thorough index for the course. And you'll still be reading plain English.

All in all, we believe that the new *EISM* is more readable and user-friendly than ever.

To enroll, just complete a DA Form 145 (available from your Cog Office) and send it to the Army Institute for Professional Development (IPD). The address is on the form.

REVISED *PSCD* AVAILABLE THIS FALL

Protecting SECRET and CONFIDENTIAL Documents, DS 2104, is the follow-on to the *EISM* course Like *EISM*, *PSCD* is being aligned with the new *ISM* and is being reformatted.

Development of the new *PSCD* is nearly complete, and most of it is undergoing a final review. We expect that it should be ready to go to the printer at the end of September, and that it should be available for enrollment in late October or early November.

Pending receipt of the new edition, IPD has suspended enrollment in *PSCD*. So those who are planning to enroll in *PSCD* should wait to apply until the new edition is available.

Security Awareness Publications Available from the Institute

Postage Requirement: We ask that you provide postage, but the publications are free of charge. Instructions for figuring postage are provided on the next page. See ordering instructions below.

To Order:

1. Check publications on the list below.
2. Add total weight. Include 1 oz. for envelope.
3. Figure the postage using information on the next page.
4. Choose envelope size (see chart 4, next page); affix postage and mailing label.
5. Send this page with **stamped** (no checks, please), self-addressed envelope to:

DoD Security Institute
Attn: EPD
c/o DGSC
Richmond, VA 23297-5091
(804) 275-5314 or AUTOVON 695-5314

(TAS) Training Aids for Security Education. June 1991. Catalog of audiovisual and printed material of interest to security educators. Instructions for ordering . . . . . ___ 3.5 oz.

(REC) Recent Espionage Cases: Summaries and Sources. June 1991. Seventy-eight cases, 1975 through 1989. *"Thumb-nail" summaries and open-source citations* . . . . . ___ 3.5 oz.

(FIT) The Foreign Intelligence Threat to U.S. Defense Industry. By Defense Security Institute staff. January 1991. . . . . ___ 3.0 oz.

(FTB) Foreign Travel Briefing. 1981. Script of briefing designed for cleared employees traveling to designated countries. Outlines methods used by hostile intelligence services and precautions against them. (For 14-minute tape/slide briefing, see "Training Aids for Security Education.") . . . . . ___ 2.5 oz.

(SIT) Soviet Intelligence Targeting of the US Scientific Community, August 1990. A basic tutorial for those in contact with the Soviet scientific community . . . . . ___ 3.0 oz.

(CUT) Control of Unclassified Technical Data with Military or Space Application, May 1985. DoD 5230.25-PH. 20-page booklet prepared by the Office of Secretary of Defense explaining the DoD program to limit public disclosure of export-controlled technical data and the special markings for technical documents. . . . . ___ 1.5 oz.

(SAM) Soviet Acquisition of Militarily Significant Western Technology: An Update, September 1985. Western products and technology secrets are being systematically acquired by intricately organized, highly effective collection programs . . . . . ___ 5.5 oz.

Individual back issues of the *Security Awareness Bulletin* up through #2-89 are no longer available from the Institute. Reprints of past feature articles have been brought together under a single cover in a publication, *Security Awareness in the 1980s.* Available from the Government Printing Office, stock number 008-047-00394-3. Price is $11.00. To order call (202) 783-3238.

Security Awareness Bulletin. Back issues available as indicated.

(1-90)	Oct 89	Foreign Travel. FOR OFFICIAL USE ONLY.	___ 3.0 oz.
(2-90)	Jan 90	The Case of Randy Miles Jeffries	___ 3.0 oz.
(3-90)	Apr 90	Beyond Compliance – Achieving Excellence in Industrial Security	___ 5.5 oz.
(4-90)	Aug 90	Foreign Intelligence Threat for the 1990s	___ 3.5 oz.
(1-91)	Jan 91	Regional Cooperation for Security Education	___ 3.5 oz.
(2-91)	Sep 91	AIS Security	___ 3.5 oz.
		Allow for envelope	✓ 1.0 oz.

Total weight . . . . . ____

Send postage in the amount of . . . . . $_____

Postage Information

If total weight is **11 ounces or less:**

Chart 1: find the amount of postage

Example: If total weight is 4.5 oz., postage is $1.21.

Chart 1

Weight not exceeding:	First Class Rate
1 oz.	$0.29
2 oz.	0.52
3 oz.	0.75
4 oz.	0.98
5 oz.	1.21
6 oz.	1.44
7 oz.	1.67
8 oz.	1.90
9 oz.	2.13
10 oz.	2.36
11 oz.	2.59

If total weight is **greater than 11 ounces:**

Chart 2: find postal zone using first 3 digits of your ZIP code

Chart 3: determine amount of postage using weight and zone

Chart 2 Postal Zone Chart

ZIP Code Prefixes	Zone	ZIP Code Prefixes	Zone	ZIP Code Prefixes	Zone
004-005	3	295	3	513-560	5
006-009	7	296	4	561-576	6
010-043	4	297	3	577	7
044	5	298-322	4	580-585	6
045	4	323-325	5	586	7
046-047	5	326	4	587	6
048-065	4	327-349	5	588-593	7
066	3	350-353	4	594	8
067	4	354-355	5	595	7
068-119	3	356-359	4	596-599	8
120-126	4	360-361	5	600-608	5
127	3	362	4	609	4
128-147	4	363-367	5	610-617	5
148-163	3	368	4	618-619	4
164-165	4	369	5	620-667	5
166-172	3	370-374	4	668-672	6
173-174	2	375	5	673	5
175-196	3	376	3	674-693	6
197-223	2	377-379	4	700-705	5
224-225	1	380-383	5	706	6
226	2	384-385	4	707-729	5
227	1	386-397	5	730-742	6
228-229	2	399-410	4	743-744	5
230-232	1	411-412	3	745-748	6
233-237	2	413-414	4	749	5
238-239	1	415-416	3	750-754	6
240-241	2	417-418	4	755	5
242-243	3	420	5	756-784	6
244-245	2	421-436	4	785	7
246-253	3	437-439	3	786-796	6
254	2	440-443	4	797-831	7
255-266	3	444-447	3	832-844	8
267-268	2	448-455	4	845	7
270-274	3	456-457	3	846-864	8
275-279	2	458-496	4	865-885	7
280-286	3	497-509	5	889-999	8
287-294	4	510-512	6		

Chart 3 Priority Mailing Rates by Zone

Weight, up to --	*1, 2, 3*	*4*	*5*	*6*	*7*	*8*
2 lbs.	$2.90	$2.90	$2.90	$2.90	$2.90	$2.90
3 lbs.	4.10	4.10	4.10	4.10	4.10	4.10
4 lbs.	4.65	4.65	4.65	4.65	4.65	4.65

Chart 4 Envelope Size

Publications measure 8 1/2 x 11"

No. of pubs	envelope
1-9	9 1/2 x 12"
10-18	10 x 15"