March 1994/Number 1-94

security awareness bulletin

Inside:

Research on Espionage

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

The Security Awareness Bulletin is provided by the Department of Defense Security Institute, Richmond, Virginia. 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 education methods.

New distribution, address changes:

Government agencies: DoD Security Institute, Attn: SEAT, 8000 Jefferson Davis Hwy, Richmond, VA 23297-5091, POC Del Carrell, (804) 279-5314, DSN 695-5314; fax (804) 279-6406, DSN 695-6406.

DIS activities: HQ DIS/V0951, 1340 Braddock Place, Alexandria, VA 22314-1651.

DISP contractors: Automatic distribution to each cleared facility. Send change of address to your DIS field office.

Espionage: Why Does it Happen?

The Department of Defense and the Intelligence Community have been taking a hard look at the possible causes of espionage and the betrayal of public trust. The results of systematic research have important implications for protecting the nation's secrets and critical technologies.

By Lynn F. Fischer,
DoD Security Institute

Since World War II, perhaps going back to the time of the Rosenberg case,[1] there has been a lot of conventional wisdom about why people commit espionage and what personal characteristics might be clear predictors of involvement in this crime. Views on this subject have changed over the past several decades, but only recently have federal agencies begun to engage in serious research regarding its root causes or reliable indicators.

At one time, it was commonly believed that *ideology*, particularly of the communist brand, was behind the thinking of espionage offenders. And in fact, during the 1950s a number of spies were communist sympathizers. Another bit of conventional wisdom held that most were foreign implants, that is deep-cover agents or moles, and therefore might be spotted by their Slavic accents, foreign associations or odd way of dress. And then there were those who were convinced that many spies were homosexuals, a connection recently downplayed by former Secretary of Defense Cheney as "an old chestnut." By the 1980s, it became evident that most spies were volunteers rather than foreign agents or Americans recruited by foreign agents. And in recent years, security educators have promoted the theory that nearly all of these offenders did it for money—for greed or because they were faced with overwhelming financial problems.

A call for policy based on scientific evidence:

Interestingly enough, one can find examples from the history of espionage in the United States that seem to confirm any of these theories, particularly the latter. On the other hand, there are cases that contradict any preconception about who would be a bad security risk. In determining whom we can trust to protect our secrets, what guidelines are appropriate? Should personnel security policy be based on common sense or in what appears at the time to be self-evident truth? In a major turning point, the 1985 Stilwell Commission Report called for such policies to be grounded on hard evidence and the scientific method:

> "Adjudication policies also beg for a firmer basis in research. DoD guidelines for denying security clearances should logically be based upon a credible analysis which demonstrates a logical link between the grounds used for denying a security clearance (e.g., excessive use of alcohol) and the likelihood that such behavior may reasonably be expected to lead to a compromise of classified information."

The report went on to call for more funding for security research in a number of areas including "determining the efficacy of the elements of background investigations, including information required on personal history statements and in subject interviews." Consider the historical context of this report: By 1985, the number of new espionage cases coming to light were nearly a dozen a year, not the least of which was the Walker Spy Ring and the untold damage in its wake. Many of the culprits arrested held high level security clearances. Political leaders and the press were seriously questioning the effectiveness of our security clearance procedures.

Responding to the Stilwell challenge:

The Stilwell recommendation did happen. By 1986, PERSEREC, the Personnel Security Research Center in Monterey, California, with several full-time government researchers and contract support was up and running. One of PERSEREC's first research efforts was to develop an unclassified database on all Americans involved with espionage against the U.S. since World War II based on media reports, trial records, and unclassified official documents.

One might ask how a massive accumulation of facts about these espionage offenders would bring us closer to an understanding of this crime and what causes it.

[1] *Ethel and Julius Rosenberg convicted of espionage for passing atomic secrets to the Soviets were executed in 1953.*

We knew a lot about each individual case from detailed investigative reports that followed the event. But it was difficult to make sound generalizations about this type of behavior without data on a wide range of variables for as many cases as possible. One of the things that made a rigorous study of espionage somewhat difficult was that, despite its tremendous damage, classic spying on behalf of a foreign intelligence service is a relatively rare crime. Since 1945 to the present there have been fewer than 120 acknowledged espionage cases which have appeared in open sources.

But even with fewer than 120 cases, an existing database of information has made it possible to systematically collect, quantitatively code, and statistically analyze basic information. This includes such things as personal background, the methods and motivations of the offender, and pertinent facts about the crime itself—situational features, what was lost or compromised, and consequences for the subject. For example, we might want to know what sort of people have been arrested, why they did it, how they got involved, what if anything they were paid, or what foreign interest received (or was intended to receive) the information.

Answers to these and many other questions are included in PERSEREC's May 1992 report, *Americans Who Spied Against Their Country Since World War II.* That report analyzed 117 cases, the number in the database as of June 1991. This report shows for each of 56 variables (such as age, gender, occupation, or motivation) the percentages of individuals who fall into one of several categories.

Some examples of the report's statistical analysis follow. These tables allow us to examine the frequency distribution for one variable at a time or to make comparisons among variables. The inclusion of a large number of cases is important in research of this type since the larger the number of cases we can observe, the greater is our confidence in the generalizations we can make on the subject.

The example at the top of the next column illustrates one way in which these data are displayed in the PERSEREC report. We can see here that by far the greater number of offenders initiated the activity themselves (usually by contacting foreign representatives). Of the remainder, fewer than a fourth were recruited by foreign intelligence agents.

It is also possible to spell out the relationship between two variables with a cross-tabulation. The next table shows that among espionage offenders who were in the military, about two-thirds began their involvement before the age of 30, while among civilians; initial offenders tended to be older. This difference probably is a result of the simple fact that the military population has a lower average age, but it does remind us that security awareness products used in military organizations should appeal to younger adults.

Volunteer and Recruited Spies

Volunteers and Recruits	%	N
Volunteers	62.9	73
Recruited by family or friends	14.7	17
Recruited by foreign intelligence	22.4	26
Total	100.0	N = 116
		Missing = 1

Perhaps the most important section of the PERSEREC report looks at motivations for espionage cross-tabulated with other variables. Were, for example, volunteer spies seeking other rewards than recruited offenders? The table at the top of the next page compares three categories of spies with regard to reported motivations:

According to this evidence, financial gain played a much larger role among volunteers (almost 60%) than among those who were recruited. Not surprisingly, those recruited by family or friends were more often

Age Espionage Began by Military and Civilian

Age	Military %	Military N	Civilian %	Civilian N
20	8.3	5	1.8	1
20-24	38.3	23	17.9	10
25-29	20.0	12	21.4	12
30-34	13.3	8	14.3	8
35-39	13.3	8	10.7	6
40-44	6.7	4	17.9	10
45 +	0.0	0	16.1	9
Total	100.0	60	100.0	56
Median	25.3		32.6	

N = 116
Missing = 1

motivated by ingratiation (the desire to favor or satisfy) than by anything else. However, it must be pointed out that at least 34 spies out of the total had mixed motives for what they did, and in those cases, it is often difficult to determine which driving force was dominant.

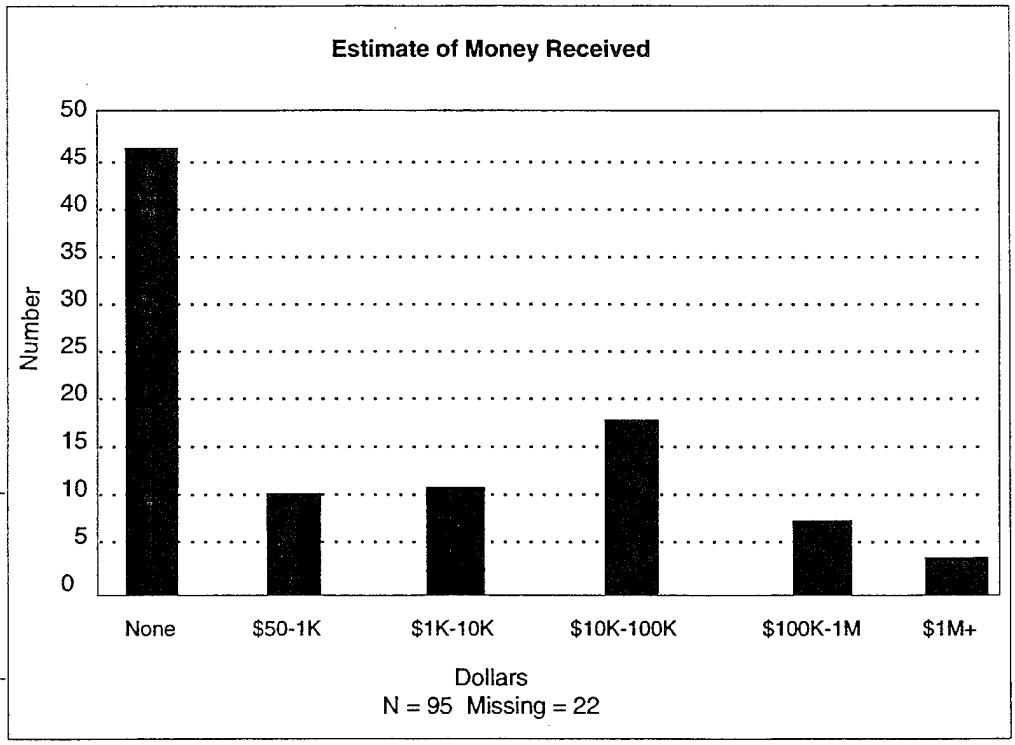
Motivation of Volunteer and Recruited Spies

Motivation	Volunteers		Recruited by Family or Friends		Recruited by Foreign Intelligence	
	%	N	%	N	%	N
Money	59.6	56	29.2	7	45.2	14
Ideology	8.5	8	25.0	6	22.6	7
Disgruntlement/Revenge	18.1	17	4.2	1	9.7	3
Ingratiation	6.4	6	41.7	10	0.0	0
Coercion	0.0	0	0.0	0	12.9	4
Thrills/Self-importance	7.4	7	0.0	0	9.7	3
Total	100.0	94	100.0	24	100.0	31

N = 150*

*More than the number of spies because there were 34 spies with multiple motivations.

Although money appears to top the list of motivations attributed to these offenders by the report, it is interesting to see (as shown in the following bar chart) how few received any significant amount of payment for these activities before being arrested. Almost half received nothing because of early detection or because they acted from non-mercenary motives. Only ten received $100,000 or more—usually paid over long periods of time. This is important information for the security educator to communicate to employees. In most cases, the financial pay-off to the espionage offender is nil or next to nothing, when compared to the monumental cost to the nation from compromised weapon systems, lost technology lead-time, or neutralized intelligence collection systems.



Here are a few additional highlights from the report's tables and descriptive findings that give us additional understanding about motivations and situational factors:

- The percentage of offenders who were volunteer spies (not recruited) has increased sharply each decade since the 1950s, reaching 79% in the 1980s.
- Forty offenders out of the total number had close foreign relatives, and spies with foreign relatives were much more likely to have been recruited by foreign agents than those who had none.
- Money tops the list of apparent primary motivations for espionage with 52%. Others include

ideology (18%), disgruntlement or revenge (15%), ingratiation (9%), coercion (4%) and thrills or intrigue (3%). *But money as a motivation can mask much more complicated motives.*

- Ideology was the dominant motive in the 1940s (12 cases); there have been only nine cases based on ideology since then.

- Out of 117 individuals, 6 were homosexual, 86 heterosexual, and the sexual orientation of the remaining 25 was unknown. The report states that homosexuality was not a significant factor in any of the cases.

- Thirty-nine offenders were known to have been involved in drug or alcohol abuse; those who were intercepted before information was lost were more likely to be substance abusers.

- Volunteer spies were more likely to fail in their effort to pass information to foreign interests. Forty-four percent were caught in the act whereas only 7% of the recruited spies were intercepted before they could damage national security.

Any of these findings may have implications for both policy and security awareness activities. The fact, for example, that since 1945 a large number of former spies had foreign family connections suggests that employees with foreign emotional ties should be informed that adversarial intelligence services have in the past used this as a leverage for recruitment. But overall, the predominance of volunteer spies (as compared to recruited sources) should lead us as security educators to stress the importance of continuing evaluation at least as much as, if not more than, recruitment *modus operandi* of foreign agents. Another example from the PERSEREC study, worth promoting to our employee populations, is that the high percentage of offenders who were also substance abusers (out of proportion to the general employee population) suggests that drug use and alcoholism should be taken very seriously as an indicator having implications for security.

There are of course many other interesting percentage distributions and comparisons between variables that may shed light on espionage and how to combat it. For one thing, it may now be possible to compare espionage with similar betrayal of trust behaviors—embezzlement, white-collar crime, industrial espionage, computer crime, or police corruption. This raises the question: Is espionage a really unique type of wrongdoing committed by quite different types of people or is it just one variation of betrayal-of-trust behavior? The verdict is still out on that question. And, on the policy side, with this database we can check out specific propositions about situational or personal traits such a drug use, alcoholism, or sexual misconduct as possible indicators of security risk. This information may eventually help to validate or downgrade the importance of specific investigative criteria used as the basis for granting clearances.

PERSEREC's Espionage Database is being updated and its holdings expanded. As new cases are added to the file and previously missing data filled in, the database becomes increasingly valuable as an information resource to the security community. In a related research effort, PERSEREC analysts are now compiling a much larger collection of cases related to the illegal export of critical technology to foreign interests.

Espionage research from another perspective

The PERSEREC effort to decipher the mysteries of espionage is not the only research activity of its type which is providing valuable results. At the other end of the continent, in Newington, Virginia, several federal agencies have pooled their resources to support the *Community Research Center*. The CRC as a research effort has actually been going strong for several years under the name *Project Slammer*, but only recently has it acquired full-time staff members and permanent office-space.

The driving concept behind *Slammer* is that if we want to know why people commit espionage, we should ask those who have done it. In other words, understanding the behavior by going directly to the perpetrators for information. On the surface, this is a simple idea, but as a research method for collecting valid information there are a number of hurdles to overcome. One of them is that most of these offenders are in maximum security prisons (hence the name, "Project Slammer") and some are unwilling to talk . Of the thirty who have agreed to be interviewed to date, each has participated in several hours of psychological testing and in-depth discussions with one or more clinical psychologists and counterintelligence specialists associated with the project. Using both standard interview forms and recorded videotapes, interviewers have recorded information on a wide variety of personality, behavioral, and situational factors as well as on espionage tradecraft. Each full interview is taped and coded for later retrieval when specific research questions need to be answered.

There are several important differences that separate the *Slammer* project from PERSEREC activities.

For one thing, the former is dedicated exclusively to the study of espionage behavior and its causes. For PERSEREC, espionage research is only one of many projects related to the entire field of personnel security. (A selected listing of PERSEREC research reports which can be ordered is included in this issue.) A second important distinction is that while PERSEREC's findings rest on the statistical analysis of quantitative data on a large number of variables or indicators, *Project Slammer* seeks valid conclusions from a qualitative, in-depth case study analysis of information on a smaller (but continually growing) selection of offenders. And when thoroughly dissected, these studies may tell us more about the intricate psychological factors, perceptions, and emotions leading to the tragic decision to betray one's own country. An important part of each data set is drawn from the individual's recall of childhood events and pre-adult behavior that tell us a lot about his psychological and emotional development and mental health.

These in-depth *Slammer* studies can also tell us about the situational context in which espionage was committed. For example, what was going through the mind of an offender at the time: Did he consider the probability of detection, was he aware of penal consequences if caught, did he see anything standing in the way of this action in the workplace, and what were his immediate objectives for resorting to this act?

To date, the research staff at *Project Slammer* has issued a number of reports—many of them are highly technical or classified—which makes it impossible to discuss their content here. In addition, much of the published output has been developed to address counter-intelligence or investigative issues not specifically of interest to the security educator or cleared employee. However, copies of *Project Slammer* reports will soon be available also through the Defense Technical Information Center and will be announced in the *Security Awareness Bulletin.* Report topics will include psychological profiles of individual spies, why people commit espionage, monitoring and continuous evaluation, evaluation of suitability criteria, and managing at-risk employees.

The *Countering Espionage* Video Series

What may be of greater interest to those of us who are committed to security education and awareness is a parallel effort by the CRC to develop, in conjunction with the Department of Defense Security Institute, a series of video products. These videos are based (as is the research effort) on the recorded testimony of convicted espionage felons in which they reveal their thinking and personal suffering. The *Countering Espionage* series has already produced one award-winning product, "You Can Make a Difference," and several more are nearing completion. The second one to be released, "It's Not a Victimless Crime," will concern the personal damage done by espionage to the offender and to his family members. A listing of titles and anticipated release dates for these products are seen in the following box.

The Countering Espionage Video Series

Title	Classification	Anticipated Release date
You Can Make a Difference	Unclassified (FOUO)	Completed and being distributed
It's Not a Victimless Crime	Unclassified (FOUO)	FY 1994
On Becoming a Spy	Unclassified (FOUO)	FY 1994
Damage to the Nation	Secret	FY 1994
How Spies are Caught	Secret	FY 1995
Security Indoctrination	To be determined	FY 1995
Security Beyond the Exit Briefing	To be determined	FY 1995

In these video productions we are attempting on one hand to dispel misconceptions, and on the other, to motivate and empower all employees and service personnel to get involved in the continuing evaluation process by intervening on behalf of troubled co-workers when they see signs of extreme stress or other indicators. The argument here is that intervention may take the form of personal confrontation, counseling, employee assistance programs, or reporting in confidence to a security professional. Whatever response is most appropriate, each of us has a personal responsibility to act in the interest of a friend or co-worker who is showing signs of not being able to cope with an immediate situation or life-crisis. This idea is very similar to the admonition that "friends don't let friends drive drunk." In this context, our message is "don't let friends or co-workers become so vulnerable that they might resort to some desperate act."

Working toward a Theory of Espionage

Will it ever be possible to predict with any degree of accuracy who might commit espionage? Perhaps not, but through research we are moving to a much better understanding of the motivations or causal factors which entrap people into this web of crime. According to Dr. Neil Hibler, *Project Slammer* Director, our hope for the future is that we at least will be able to identify "at risk" individuals before or during employment, thus *preventing* espionage or compromise by cost-effective policies which are at the same time harmonious with human values and constitutional principles.

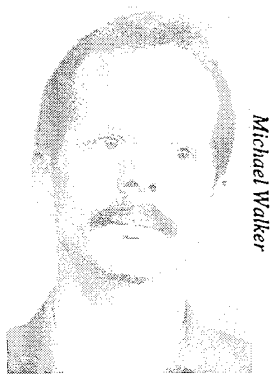
For the present we must try to make some sense out of the sizable array of information collected on these cases by both the PERSEREC and *Slammer* research efforts. At first assessment, the facts seem to defy our efforts to generalize about motivations or causes. It could almost be said that each instance of this crime is a unique event in itself—each has its own twists and exceptional personalities. Each account reveals another variation on the old theme of personal failure and betrayal.

However, CI professionals and psychologists working on the *Slammer* data tell us that common patterns are beginning to emerge. The results of psychological testing and interviewing disclose that they frequently encounter two, almost opposite, personality types among these 30 offenders under study—one, a highly manipulative, dominant and self-serving type; the other, passive, easily influenced and lacking in self-esteem. Anyone who is at all knowledgeable about recent cases will immediately think of spy ring organizers such as John Walker and Clyde Lee Conrad as typical of *wheeler-dealers*. Walker's son, Michael, comes to mind as a likely candidate for the *wimp* category. *Project Slammer* researchers tell us that by far the larger number of former spies in their sample fall into the first group, but contrary to what we might expect, none of the subjects studied entered a position of trust with the intention of committing espionage.

We also learn from CRC's report on personality characteristics of espionage offenders [soon to be available from DTIC] that a frequent trait among this group is obsessive self-centeredness or selfishness—a lack of genuine caring for others and an indifference to problems experienced by other persons.

But the larger issue is this: What would lead even a person who is lacking in a basic sense of loyalty or sympathy for others to opt for espionage, which most of us would conclude is a highly risky and ultimately self-destructive act? The answer is complex, but we *can* make sense of what is going on. These researchers are finding that in case after case they are looking at a person who is psychologically vulnerable to begin with and whose judgment under stress may be severely impaired. Following employment in a sensitive position, and when confronted with a high level of emotional pain, frustration, or anger, in desperation he or she resorts to espionage as a way out or as a solution to a problem. It may be a one-time act such as the theft of a single CIA manual by William Kampiles, or repeated acts of betrayal over months or even years, as reported in the case of former Army Warrant Officer James Hall.

The nature of the espionage offender's vulnerability to involvement in this crime, or any other damaging behavior, differs from case to case. We do know that several of these people were victims of severe child abuse which resulted in an intense self-esteem problem. Others appear to have been raised without the benefit of moral training or positive role models. In his cell at the Federal Penitentiary at Lewisburg, Pennsylvania, Michael Walker told us:



Michael Walker

"...my father got me involved in espionage through years of careful grooming. The way you train a man to think, a young man to think about values, morals, and things like that. These are important. If you can convince your child that certain things are okay, they're

more inclined to break certain rules in society."

Does this mean that anyone who has emerged from a dysfunctional or undesirable family background is going to attempt espionage? Definitely not. The idea driving this project was to try to understand why those who *have* committed this crime went in that direction when they found themselves in what they believed to be an intolerable situation. The "crisis" or compelling circumstance in the lives of these offenders turns out to be as varied as the origins of their vulnerabilty or predisposition to destructive behavior. Several individuals faced mounting debts and personal bankruptcy, some craved professional recognition, one was a covert homosexual who bitterly resented military policy. In another case, Thomas Dolce, an Army civilian employee with a history of psychiatric problems directly links his espionage activity with domestic tragedy:

> "I had seen a psychiatrist off and on for about three years. I had been in, not a psychiatric hospital, but in a psychiatric wing of a general hospital three or four times. I had been on some heavy medication and so on. I was a real mess for about three years. Roughly two years after that, for whatever that means, is when all of this started—shortly before or shortly after this [espionage activity] started—I'm not sure which, but my mother died very suddenly. And I think that I did not fully appreciate at the time just what the impact of that was. I think I've come to appreciate that more in the last year—the impact that it had on me. Roughly a year after my mother died, my late wife was diagnosed as having cancer. And we both suffered with that for about three years before she died. It was during those three years that the bulk of the activity took place."

As with psychological vulnerability, these findings should not suggest that employees confronted with a life-crisis will necessarily select espionage, or any self-destructive act as an option. But on the other hand, they are at much greater risk. It is important to emphasize again that, by comparison with other felonies, espionage doesn't happen that often. We know that only a tiny fraction of people under stress—who think they are up against the wall—would even think of espionage as a remedy for anything. Call it basic loyalty, patriotism, or morality; in most cases, overriding values would rule it out. However, for those few who did go over the line, this new research also shows that they rarely considered themselves to be disloyal. We can assume that this rationalization is related to their typical, self-centered view of life.

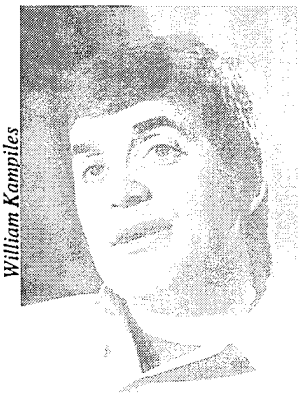
Long-term benefits from research on espionage

Then how will the results of these research ventures described above assist us in protecting the nation from the loss of critical information and technology by theft, negligence or betrayal? *First*, in the area of initial screening for access to classified or sensitive information, we stand to learn in the future a lot more about what makes an individual vulnerable, or a higher risk, and what does not. Much of the on-going work of both PERSEREC and the Community Research Center is related to the evaluation of the current investigative criteria for suitability to hold a clearance—foreign connections, drug abuse, sexual misconduct, illegal activities, etc.

Each of these complementary research efforts is in its own way providing insight into aspects of the larger issue of predicting human reliability in government personnel security programs. For example, while both research projects report a high incidence of habitual and excessive drug and alcohol use among espionage offenders (clearly a suitability issue), *Project Slammer* researchers call attention to their data which indicate that substance abuse was not typical of offenders during the time they were in a position of trust. It may have happened before or after.

Secondly, and this may be the more immediate benefit, in the area of prevention following the granting of access: The chief conclusion drawn from several of the *Slammer* reports is that had procedures been in place to help vulnerable employees deal with personal crisis, including an organizational climate supportive of co-worker intervention, much of this damage would have been prevented. As related by former CIA employee William Kampiles, even something as simple as personal counseling might have deflected him from his single but extremely damaging criminal act:

> "...if someone outside that office had sat me down and...just said, listen this is a talk. You can say whatever you want. Nothing to hide. Nothing will leave this room. Tell us what's going on in your life, because there's obviously a problem. You're not doing well, you know, you're not communicating in a positive manner. Your relationships with your co-workers are bad... what's going on?...we don't think that this is what you want. It's not what's been



William Kampiles

demonstrated in the past in your life. Is there anything that we can do to help?"

Research Impact: Of immediate importance to security education

Lastly, for the security educator, much is to be gained from keeping fully informed about what espionage research has to tell us. "Findings" that are clear and easy to understand, such as the fact that most of the damage in recent years has been the result of volunteer U.S. citizens rather than recruited or foreign spies, is useful information to plug into awareness briefings. And as mentioned earlier (based on the PERSEREC study), the potential extra vulnerability of employees with foreign relationships, and the high incidence of substance abuse in the offender population are pertinent issues to discuss in briefings and open forums.

Project Slammer findings offer us some of the best verbal ammunition available for promoting the concept of co-worker responsibility and continuing evaluation. Through these research efforts, we are learning that people who have fallen into the trap of espionage are like the guy in the next office or the trusted technician on the assembly line. As mentioned earlier, no offender studied so far has entered into a position of trust with the intention of betraying that trust. Among convicted Americans who had held a clearance, involvement with espionage happened following initial employment, sometimes years later.

This focus on the active role of rank-and-file employees in preventing espionage is reinforced by another revelation: Many of the former spies claim that their decision to commit this crime was based in part on their belief that the probability of being noticed and reported by co-workers was next to nothing. In other words, the messages for our audiences to hear are: Intervene in the interest of an at-risk employee before he or she becomes a threat to national security. And secondly, a workplace in which people are known to be aware and willing to take action when appropriate presents a powerful deterrent to espionage.

Through security education, we also need to clear the deck of misconceptions. Not the least of these is the idea that reporting in confidence about a co-worker is going to be detrimental to that person. Several of the former spies, such as William Kampiles, have said that they wish someone *had* stood in their way. Statements like this help support our arguments that personal intervention is morally and ethically justified as being consistent with the interest of a co-worker who is exhibiting signs of distress or the inability to cope with a situation.

These central themes are developed in the *Countering Espionage* video series. And as these products are released, our employee populations will have the opportunity to witness for themselves the testimony of former spies. Through comprehensive security awareness programs—briefings, videos, newsletters, posters and other visual reminders—we can create a climate in which people are sensitive to trouble signs and feel morally empowered to act. And at the same time we are building a deterrent atmosphere where the potential offender will assess the chance of detection as too high.

Over all, the credibility of our personnel security programs depends upon a great "selling-job" by the security educator through effective briefings and other communications. And our credibility as communicators and educators stands to be greatly enhanced each time we are able to say, "What we are telling you is not just common sense, but this has been validated by scientific research."

PERSEREC Publications
1987-1993
(DTIC reference numbers included)

Revision of adjudicative criteria for alcohol and drug abuse, and emotional/mental disorders — **DTIC AD-A249 448**

Bosshardt, M.J., & Crawford, K.S. (1992). (PERS-TR-92-003)

Continuing assessment of cleared personnel in the military services: Report 1—A conceptual analysis and literature review — **DTIC AD-A234 280**

Bosshardt, M.J., DuBois, D.A., & Crawford, K.S. (1991). (PERS-TR-91-001).

Continuing assessment of cleared personnel in the military services: Report 2—Methodology analysis, and results — **DTIC AD-A234 281**

Bosshardt, M.J., DuBois, D.A., Crawford, K.S., & McGuire, D. (1991). (PERS-TR-91-002).

Continuing assessment of cleared personnel in the military services: Report 3—Recommendations — **DTIC AD-A234 282**

Bosshardt, M.J., DuBois, D.A., & Crawford, K.S. (1991). (PERS-TR-003).

Continuing assessment of cleared personnel in the military services: Report 4—System issues and program effectiveness — **DTIC AD-A234 283**

Bosshardt, M.J., DuBois, D.A., & Crawford, K.S. (1991). (PERS-TR-91-004).

The investigative interview: A review of practice and related research — **DTIC AD-A235 851**

Bosshardt, M.J., DuBois, D.A., Paullin, C., & Carter, G.W. (1988). (Institute Report No. 160). Minneapolis, MN: Personnel Decisions Research Institute.

Personnel security prescreening: An application of the Armed Services Applicant profile (ASAP) — **DTIC AD-A207 147**

Crawford, K.S., & Trent, T. (1987). (PERS-TR-87-003).

Screening enlisted accessions for sensitive military jobs — **DTIC AD-A210 159**

Crawford, K.S., & Wiskoff, M.F. (1988). (PERS-TR-89-001).

Development of user-friendly credit reports — **DTIC AD-A241 654**

Duckworth, D., & Rubenking, B. (1990). Bethesda, MD: Booz, Allen & Hamilton.

Moral waivers as predictors of unsuitability attrition in the military — **DTIC AD-A210 160**

Fitz, C.C., & McDaniel, M.A. (1988). (PERS-TR-88-006).

Due process in matters of clearance denial and revocation: A review of the case law by John Norton Moore, Esq., Ronald L. Plesser, Esq., and Emilio Jaksetic, Esq. — **DTIC AD-A206 217**

Haag, E.V., & Denk, R.P. (1988).

Beyond compliance: Achieving excellence in defense industrial security — **DTIC AD-A219 906**

Haag, E.V., Crawford, K.S., Riedel, J.A., Wood, S., Schroyer, C.J. (1990). (SR-90-001).

Alcohol use and abuse: Background information for security personnel **DTIC AD-A242 156**
Heuer, Jr., R.J. (1991). (PERS-TR-91-010).

Financial irresponsibility: Background information for security personnel **DTIC AD-A242 155**
Heuer, Jr., R.J. (1991). (PERS-TR-91-011).

Compulsive gambling: Background information for security personnel **DTIC AD-A252 301**
Heuer, Jr., R.J. (1992). (PERS-TR-92-006).

Crime and security risk: Background information for security personnel **DTIC AD-A269 733**
Heuer, Jr., R.J. (1993). (PERS-TR-93-005). Defense Personnel Security Research Center.

Issues developed in background investigations conducted by Defense Investigative Service **DTIC AD-A221 237**
Lewis, P.A.W., Koucheravy, E.R., & Carney, R.M. (1989). (PERS-TR-90-004).

Determination of training requirements: Personnel security specialists (adjudicators) **DTIC AD-A210 157**
Marshall-Mies, J. (1987). (HumRRO 87-02). Alexandria, VA: HumRRO International.

Job/task analysis for DoD adjudicators Phase A: Job tasks for DoD adjudicators **DTIC AD-A221 250**
Marshall-Mies, J., Rigg, K., & Harding, F. (1989). (HumRRO 88-04). Alexandria, VA: HumRRO International.

Vanity-motivated overspending: personnel prescreening for positions of trust **DTIC AD-A262 383**
Morris, S.B., McDaniel, M.A., Worst, G.J., & Timm, H. (1993). McLean, VA: Booz-Allen & Hamilton.

Temperament constructs related to betrayal of trust **DTIC AD-A249 985**
Parker, J.P., & Wiskoff, M.F. (1991). (PERS-TR-92-002).

Security awareness training and education (SATE): A survey of DoD installations **DTIC AD-A257 908**
Parker, J.P., Riedel, J.A., & Wiskoff, M.F. (1992). (PERS-TR-92-007).

Development of the Marine security guard Life Experiences questionnaire **DTIC AD-A216 140**
Parker, J.P., Wiskoff, M.F., McDaniel, M.A., Zimmerman, R.A., & Sherman, F. (1989). (PERS-TR-89-008).

Prescreening military officer candidates for high level security clearances **DTIC AD-A212 737**
Rosenthal, D.B. (1989). (HumRRO 89-02). Alexandria, VA: HumRRO International.

Homosexuality and personnel security **DTIC AD-A242 914**
Sarbin, T.R. (1991). (PERSTR-91-008).

Security awareness and public opinion, with special attention to financial and credit issues **DTIC AD-A262 047**
Smith, T.W. (1991). Chicago, IL: National Opinion Research Center, University of Chicago.

Investigative report writing: A field study **DTIC AD-A222 330**
Suchan, J.E. (1989). (PERS-SR-90-006).

Improving the efficiency of the Defense Investigative Service credit report acquisition process **DTIC AD-A225 239**
Timm, H.W. (1990). (PERS-TR- 90-005).

Personnel security and reliability: Psychological research issues **DTIC AD-A207 148**
Wiskoff, M.F. (1987). (PERS-TR-87-007).

Moral waivers and suitability for high security military jobs **DTIC AD-A208 698**
Wiskoff, M.F., & Dunipace, N.E. (1988). (PERS-TR-88-011).

Defense Investigative Service's issue case database: Analysis of issue types and clearance adjudication **DTIC AD-A225 239**
Wiskoff, M.F., & Fitz, C.C. (1991). (PERS-TR-91-006).

The child sexual abuse offender: A review of current research and implications for personnel security **DTIC AD-A206 472**
Wood, S. (1988). (PERSTN-88-002).

Americans who spied against their country since World War II **DTIC AD-A276 043**
Wood, S., & Wiskoff, M.F. (1992). (PERS-TR-92-005).

Development of a measure of vanity-motivated overspending **DTIC AD-A262 764**
Worst, G.J., Duckworth, D., & McDaniel, M.A. (1991). McLean, VA: Booz Allen & Hamilton.

Personnel security adjudicators: Results of a semi-structured interview **DTIC AD-A210 859**
Ziemak, J.P., & Laurence, J.H. (1987). (HumRRO 97-04). Alexandria, VA: HumRRO International.

Preliminary analysis of the U.S. Army Security Screening questionnaire **DTIC AD-A231 712**
Zimmerman, R.A., Fitz, C.C., Wiskoff, M.F., & Parker, J.P. (1991). (PERS-TR-91-007).

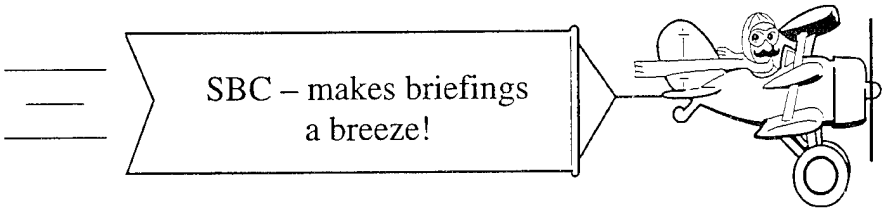
The above reports are available from the Defense Technical Information Center in Alexandria, Virginia. Government or contractor organizations must first be registered for DTIC services. To register, call DTIC's Registration Branch at (703) 274-6871 or DSN 284-6871. They will send you a registration packet and answer any questions.

If you are already registered for DTIC's services, write, fax, or phone them, giving DTIC's reference number listed immediately to the right of each entry. You may also use DTIC's Document Request Form 1, which is provided in quantity by DTIC on request.

Defense Technical Information Center
Building 5, Cameron Station
Alexandria, VA 22304-6145
Tel: (202) 274-6434
DSN 284-6434

Attention Security Educators, here's your chance to sign up for the:

Security Briefers Course!



October 4-6, 1995
Air Reserve Base, Indiana
POC: Mr. Kirk Bireley
101 Lighting Grissem
Air Reserve Base, IN 46971-5000
(317) 688-8589
DSN 928-8589

September 13-15, 1995
U.S. Air Force Academy
Colorado Springs, Colorado
POC: Angelique Phillips
Defense Investigative Service
(719) 260-1655

October 23-25, 1995
Dept. of Commerce Headquarters
Washington, D.C.
POC: your SAES representative
or Linda Braxton at DoDSI
(804) 279-6076

The Security Briefers Course will also be offered at the DoD Security Institute in Richmond on September 27-29. If interested, call Linda Braxton at (804) 279-6076.

Understanding the Computer Criminal

A paper presented at the Department of Defense Computer Crime Conference, Monterey California, 1993.[1]

by Neil S. Hibler and Jim Christy

INTRODUCTION

This report introduces our readers to a nationally-based study, currently in progress, under the auspices of *Project Slammer* . The researchers involved in this work are seeking to explain what is behind the many intentional penetrations of automated information systems and the increasingly frequent use of computers to commit crimes. They discuss the formation of this research program, the nature of information gathered, and concludes with four, brief case examples.

Among the efforts undertaken by the government to combat computer crime is a scientific study of the criminals involved. The premise of this research is that in order to develop preventive countermeasures and investigative solutions, there needs to be an intimate, insider's understanding of the crime. These efforts approach the problem from the vantage point of those most intimately aware of all that happened: the perspective of the offenders themselves. The information sought includes contributing factors such as the criminal's perceptions and explanations of how and why they committed the crime.

Developing a research model

Getting one's arms around the larger issue of computer crime requires a system by which to clearly define and categorize this type of behavior. That was our first task for, once defined, our research design could then address the question, "Why do people do this sort of thing, and how can it be prevented?" These issues affected the selection of cases which is now developing into the database from which all analyses derive.

In order to define "what" to study, a research committee was established, consisting of computer crime investigators from across the agencies of national government. This steering group prioritized their interests by two categories of issues, the mind-set of the criminal, and the spy tradecraft used.

The clear preference of the steering committee was to establish a research base from cases that showed intentional malice. In so far as tradecraft was concerned, their interest was to include cases in which information systems that are in common use were violated. We wanted to know whether there were some common techniques used. However, the driving interest was to study cases involving novel methods and/or applications. Together, these criteria are helping us to establish a database that includes the most malicious cases and those reflecting the newest violation technologies.

This initiative is also a complement to other, on-going *Project Slammer* research efforts that provide anchors for comparison to other security violations or betrayal of trust issues. For example, the established data collection procedure employed in the study of classic espionage[2] supports this computer security study by providing a methodology that has already proven to be successful. Included in the information gathered by the common structured interview protocol are details regarding the subject's life span, as partitioned by relationships, family issues, education, employment, and medical condition. One section of this inquiry details the criminal behavior, it's causes and the efforts conducted to bring it about. Further collaborative information is obtained from those who knew the subject at the time the crime was being committed. These sources include work place associates (i.e., co-workers, supervisors) as well as intimates (spouse, girlfriends, boyfriends, co-conspirators, etc.). As additional informants, they provide confirmation of subject's statements, and add their own insights as to influences on the criminal behavior

An additional source of personal information is psychological testing. In each case, standardized examination instruments were used to measure intellectual functioning and personality characteristics, to include self-esteem, social skill, and mental status. Interestingly, early

[1] *The Department of Defense Computer Crime Conference, sponsored by the Defense Personnel Security Research Center, October 1993 was attended by researchers in government and industry. Proceedings of this conference, which include a number of reports similar to this one, will be advertised in the Security Awareness Bulletin.*

[2] *By "classic espionage" we mean the theft of classified U.S. Government documents or other material and its transfer to an adversarial intelligence organization, or classified information supplied from memory to the same for whatever purpose.*

attempts to measure personality features were feared to be superficial, because often there were considerable intervals between the law-breaking behavior and testing. What the earlier research has shown is that those underlying personality traits that indicate high-risk, do not change over time. Further, these features have demonstrated considerable differences from persons who do not commit crime.

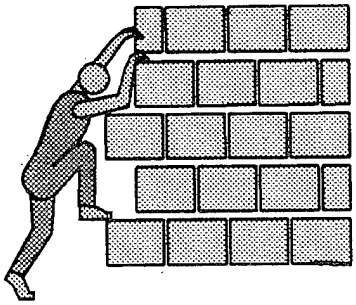
The remaining area of interest is how these subjects committed their crimes. The structured interview itself includes a section that explores the criminal acts and influences on them. Of course, both barriers and impediments to the crime are of interest; the interview protocol is the stepping off point to as full and complete an understanding as possible. In order to capture all that the subjects say, the entire interview is video taped. This "modern" aid to recording is helpful in making records that are easy to review, and are further contributed to by yet other methods of capturing and recording data.

Capitalizing on advances in simulation technology, researchers include an environmental test-bed component for observing first-hand how the crime was committed. A state of the art main frame computer has been partitioned, so that with an extensive library of software, it is possible for us to replicate the hardware and software configurations of virtually any automated information system. The resulting replicated systems are accessible by modem, allowing the subject to re-enact the crime under laboratory conditions. As he accessed the (simulated) information system, the subject's every key stroke is automatically recorded.

In total, this research effort is a collaboration between a variety of disciplines, each working closely with the other to build a better understanding of computer crime, and how to prevent and investigate it. Cases studied to date have provided many interesting details. The brief summaries that follow provide a look at some of the information that has been evaluated.

CASE EXAMPLES

Case 1. Going over the Wall



An example of low tech computer crime, this case began when a U.S. soldier decided to abandon his duty station and to defect to a foreign nation. Incidental to this plan, the soldier took with him a standard lap top computer, and two floppy disks that contained sensitive information. The disks were to provide the foreign intelligence service with his *bona fides*, as well as a (hoped for) sense of recognition and advantage.

The soldier was surrounded by various stresses. Included were persons with whom he could not get along, peers and supervisors who were critical of his work. Just the same, he had a clean record, so much so that he was scheduled to be interviewed for recognition as "Soldier of the Month." Just the same, he had great difficulty in forming effective interpersonal relationships. He had no real anchors to rely on, no one with whom to seek solace, nor to air his frustration. In his own mind, defection was an act of desperation.

This subject's knowledge of computers was so primitive that he didn't know how to copy disks, or even how to list files. He took with him the laptop computer because he didn't know if the service to which he would defect had a means to read the classified disks. He had no idea that the computer's hard drive had once held documents even more sensitive than those he stole. Unfortunately, the opposition realized what had been handed to them, they had no difficulty in recovering everything that was of value. In a surprising twist of fate, after this soldier was tried, convicted and sent to jail, he was assigned to duties in the prison library where he learned to use an MS DOS system for tracking the library's holdings. He later told researchers that if he knew then (about computers) what he knew now, he could have caused damage many times more significant. Fortunately, this subject was naive regarding computers at the time of his defection. This is very different from other cases in which the criminal had advanced knowledge, and every intent to exploit it.

Case 2. The All-American Kid

This is the story of a youthful offender who was able to conduct sophisticated violations, resulting in several hundreds of thousands of dollars damage. Beginning at thirteen years of age, he committed over two thousand computer crimes, but was arrested and convicted of only one. He admitted to using computers to gain unauthorized entry into commercial telephone com-

puter systems to find access codes and numbers. And he admitted using "phreaking" activities to eliminate long distance phone charges by using an unauthorized voice-mail system, 1-800 numbers, and customers' access card numbers. He began his illegal activity by obtaining copies of credit reports and credit card numbers. These acts perhaps, were the foreshadowing of things to come.

The subject is a hacker who explored the cyberspace networks of computers in order to communicate with other hackers. At the time of his arrest, he appeared to be an "All-American" kid. He was a high school honor student who had been awarded a full college scholarship. He worked after school, using the income to finance his computer hobby. He was described as coming from a stable home, with only minor trouble preceding his arrest. But friends considered him to be an introverted person, nearly absent in interpersonal skills.

The major reasons for this subject's illegal activity included curiosity and intellectual challenge. Hacking provided the opportunity to expand his horizons, and perhaps to overcome his social weaknesses, he used bulletin boards to relate to other hackers and to explore far away places.

CASE 3. No Stranger to the Police

This was a co-conspirator of the subject in case 2. He was also a teenager (age 16), but unlike the "honor student" profile of the preceding case, he was cocky and abrasive. Others, particularly adults, found him to be a liar who enjoyed game playing with superiors and wholly untrustworthy. He was physically small and self-conscious, but hid it with his "in your face" attitude. His parents were separated, his father was being treated for depression. The family tree also had some bad fruit. A grandfather had died in prison, having been twice convicted for armed robbery.

In so far as hacking was concerned, this subject found particular pleasure in looking at people's records; he enjoyed violating their privacy. In some instances, he wanted to cause them trouble. He would obtain credit reports, but did most of his mischief by running up telephone bills. His utmost fantasy was to enter into a computer system in which he would have the power to launch a space shuttle or to start a world war. He was so consumed by his hacking that nothing else seemed important.

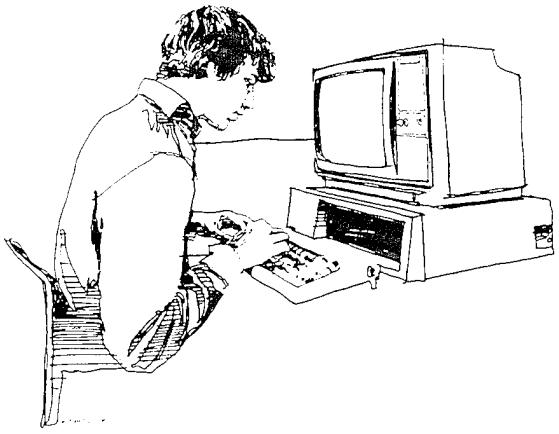
The vindictive side of this subject was almost limitless. He was proud that he was able to be disruptive. Among the intrusions he was responsible for were cancellations of garbage and water services, passing along telephone numbers of those targeted to other hackers (by placing them on a hacker bulletin board), and interrupting operating systems by removing entry access to authorized users. All of this nefarious activity was experienced without regret. To quote the subject, "If I abuse the PBX, AT&T benefits... the private owner still has to pay... AT&T gets a lot of their profit through hackers because they call illegally and [AT&T] makes other people pay for it."

He was no stranger to the police. He had been in a fight in elementary school which had to be settled by the authorities and later, when he was 14, he was arrested for stealing a car phone. A year later, his parents were contacted by the police because he was hacking into a commercial voice mail system. Security personnel from the telephone company had also reached the mother, but her only response was to yell at him.

Perhaps among the most interesting findings from this case was the generalizability of the motive to many other hacker cases. Like many others, this computer criminal did not start out with criminal intent. His introduction to the world of hacking was simply to engage in computer activities which used telephone lines, and were therefore unaffordable. His use of the computer to annoy others developed only later. He estimated that he committed over one hundred computer-assisted offenses, before being apprehended.

CASE 4. High on Hacking

Like the previous teenager, this subject suffered from learning disabilities while a child. He had been diagnosed as having Attention Deficit Disorder and for most of his elementary school years was medicated with Ritalin. In



high school his behavior problems changed in form, from being just learning inhibiting to being socially unacceptable. Despite better grades in high school, by the time this subject was seventeen he was using marijuana four times a week, and taking one to four doses of LSD one day a week. In fact, he often used drugs while hacking.

He was unreliable, but didn't see it. For instance, he had been fired from a job at a service station for suspicion of theft. He seemed to fuss about the accusation, even though he admitted to researchers that he had been skimming proceeds. He had also been arrested: Shortly before he was detained for hacking he had broken into two automobiles. His intent had been to steal something he could use to pay his rent. He plead guilty to two counts of burglary, two for conveyance of stolen property, and two for petty theft. He was on two years probation (a plea bargain) when he was investigated for his computer crimes.

While claiming he had been hacking for only nine months, his motive was ostensibly to seek out opportunities for profit; but ego needs seemed to be the force behind it all: "I felt that at some point I was going to discover something to make me wealthy, powerful or both, whether it was fraud opportunities or recruitment by a foreign or domestic power for somebody of my talents." His own attempts were initially fruitless, but he was able to hook-up with a mentor (a twenty-four year old) who taught him how to penetrate systems. Ironically, this mentor gained much of his knowledge on system vulnerabilities by keeping up to date on government-published computer security advisories.

SUMMARY AND CONCLUSIONS

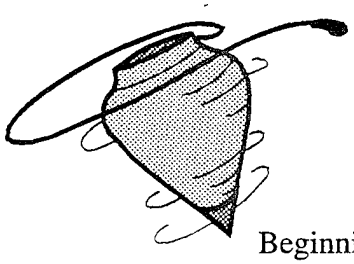
As these brief case discussions suggest, there is a great deal to be learned about computer crime by studying computer criminals. It does not appear that truly effective countermeasures or investigative procedures will be possible until there is a more complete understanding of this behavior, and in particular, situational factors that permit or deter wrong doing. The research described in this paper is still quite recent. We hope to go on to identify patterns of behavior leading to effective security countermeasures and crime prevention. To do that, the Federal government is relying on insights from the criminals themselves; it's a process that has proven to be helpful when looking at other types of criminal activity.

In working toward this goal, much is to be gained by continued cooperation among counterintelligence, security, and law-enforcement agencies. Methods of computer crime prevention, detection, and investigation should be shared among law enforcement professionals, but in ways that do not provide an advantage to a potential offender. As seen in Case 4, many of these people keep up-to-date on leading edge security technology. We need to be careful disseminators and consumers of research findings, especially those that concern the security of our own monitoring and crime fighting efforts.

Moving?

Defense industry contractors . . . If your company plans to move from its current location, let your DIS field office know your new address. That way you won't lose any issues of the Security Awareness Bulletin.

Security Program Improvement Network



by Carl Roper
Instructor, DoDSI

Beginning with the April, 1993, Security Awareness Bulletin, we have included a new column: The Security Program Improvement Network. SPIN is predicated on the fact that everyone has unique experiences, different viewpoints towards solving a dilemma in their organization. Perhaps they developed a new security product, came up with an idea that worked, or created or refined something within the security arena. SPIN provides a communications link for the "voice of experience." These lessons learned or unique accomplishments should be made available to others so that all of us can improve our security countermeasures.

Take this as an invitation to spread the word on something you have done that will help others. We're looking for anything, from a new way of doing something old that improves the end result, to a new or different computer program that has a security application. In this regard, you might tell us about a commercial program that really works, or a program developed in-house to meet a specific need. These ideas are of great value to your fellow security practitioners. Let's spread the good news about what is happening, and help each other.

"What's in it for me?" you might ask. Several types of recognition are possible in addition to getting your name and organization mentioned in the Bulletin. A little extra professional credibility could be useful in this time of downsizing and restructuring. And then there are the follow-up calls from interesting and attractive people like yourself who seek additional details and advice. Consider the networking potential!

Send your valuable ideas, comments, and examples to the DoDSI SPIN coordinator so we can publish them here. If you have come up with a new, or variation of a current, computer program, send a disk for evaluation by our AIS specialists. Samples of security education programs for a specific topic area, reports, etc., are also welcome. The better the information we receive, the more specific we can be when telling everyone else about your achievements and success.

Items should be addressed to:

Department of Defense Security Institute
Attn: SPIN Coordinator
8000 Jefferson Davis Highway, Bldg 33E
Richmond, VA 23297-5091

Customized Industrial Security Training

Tailored to meet your company's unique needs

What are the unique training needs at your facility? Let DoDSI help you meet those needs. A customized class can address the topics that are relevant to your employees.

Suggested Topics:

Personnel Security Clearances
- Electronic transmission
- DISCO
- Background investigations
- Adverse information reporting

Classification Management

Marking Classified Documents

Safeguarding Classified Information
- Storage of classified material
- In-use controls
- Closed areas
- Alarm systems

Security Education Programs
- Writing training objectives
- Developing practical exercises
- DoDSI courses available
- Other training material available

Security Violations and Compromises

Secure Telephone Unit (STU-III)
- Advantages and costs
- Procedures for acquiring a STU-III
- Training for STU-III users

Foreign Sales and Business
- Transfer of classified information
- Export controls on unclassified information and material

International Aspects of the DISP
- Cleared employees assigned outside the U.S.
- The role of DIS Office o Industrial Security International (OISI)

Hosting Classified Visits

Today's National Security Threat
- A discussion of the need to protect classified information in today's world.

Other security related topics may be included at your request.

Course length: From a few hours to 3 days. It's your call.

Customized for whom?
- managers and supervisors
- security department staff
- cleared employees
- new employees

How to schedule: Call or write

Wayne Lund
DoD Security Institute
8000 Jefferson Davis Hwy Bldg 33E
Richmond VA 23297-5091
(804) 279-3939

ISAC Update

Industrial Security Awareness Council (ISAC)

What about San Diego?

by Joanna Clevenger, TRW
Security Education Specialist

Does San Diego have an ISAC? You might have wondered when you didn't see our group mentioned in the July 1993 ISAC Network article [*Security Awareness Bulletin* 2-93]. The answer is yes, and our accomplishments have been exciting.

ISAC/San Diego acts as a clearinghouse for security education materials and creates awareness programs through its Training, SAP/SAR, Library, and Executive committees. One of our projects this year is to create a Proprietary Protection committee to study industry proprietary protection plans. Using the results of that study, we'll then create a model protection plan for local defense contractors.

Also this year we are hosting our fourth annual seminar. The theme is "Changing Concerns for the Security Professional of the 90's." The first day is entitled, "Managing Security in Change." The second day has workshops that highlight adapting security to changing policy.

We offer regular mini-seminars at no cost to attendees. Topics covered at the last two seminars were document control/accountability procedures and techniques used to gather sensitive proprietary information. Future mini-seminars planned are:

- FBI terrorist threat response in San Diego
- What to report to DIS
- STU-III procedures, and
- Teaming agreements (international considerations).

We even had a hand in establishing the ISAC at Warner Robins, Georgia. Sheila Pruitt, a TRW colleague who works in Warner Robins, heard of our success and asked for help in creating an ISAC for them. I went and talked to interested contractors, the FBI, and DIS about our group, and now *their* group has 35 members. The whole idea became contagious, and DIS asked Sheila for help in creating TRISAC, an information exchange ISAC between Georgia, North Carolina, and Tennessee.

How did our ISAC begin? Four years ago, representatives from San Diego defense contractors, DIS, and the FBI met at General Dynamics Space Systems and agreed to form an ISAC. We wanted to bolster security awareness and education by pooling the resources of the contractor and government communities. It worked. The information now exchanged through ISAC provides a better understanding among the FBI, DIS, and the defense contractor community. This increased understanding then translates into better inspections.

There are currently 12 companies represented in the ISAC/San Diego. But we consider all San Diego DoD contractor personnel to be members of ISAC, and any volunteer from the defense contractor community is heartily welcome to serve on our committees. If you want more information about our group, call one of the co-chairmen: Bob Harman, FBI DECA Coordinator, telephone (619) 557-4389; or Jim Isoda, DIS Field Chief, telephone (619) 557-5914. We're here to help you.

Schedule of Courses FY 95

DEPARTMENT OF DEFENSE SECURITY INSTITUTE

We Teach the Guardians

3/22/95

INTRODUCTION TO INDUSTRIAL SECURITY 5220.1

DoDSI, Richmond, VA
Mar 1-3, 1995
Jun 7-9, 1995
Sep 20-22, 1995

USER AGENCY INSPECTOR 5220.1A

DoDSI, Richmond, VA
Mar 6-10, 1995
Jun 12-16, 1995
Sep 25-29, 1995

INDUSTRIAL SECURITY SPECIALIST 5220.2

DoDSI, Richmond, VA
Aug 7 - Sep 14

INTRODUCTION TO STU-III 5220.3

DoDSI, Richmond, VA
Oct 6, 1994
Dec 8. 1994
Feb 27, 1995
Jun 5, 1995
Aug 10, 1995
Sep 18, 1995

Course also given at field site upon request. To host, call Wayne Lund (804) 279-3939.

FSO PROGRAM MANAGEMENT 5220.4

Oct 24-28, 1994	Boston, MA
Oct 31-Nov 4, 1994	Albuquerque, NM
Jan 24-27, 1995	Washington, DC
Feb 7-10, 1995	Los Angeles, CA
Mar 27-30, 1995	Secaucus, NJ
Apr 4-7, 1995	Dallas, TX
May 2-5, 1995	Atlanta, GA
May 9-12, 1995	San Francisco, CA
Jul 18-21, 1995	Huntsville, AL
Aug 1-4, 1995	St. Louis, MO
Aug 22-25, 1995	Washington, DC
Sep 12-15, 1995	Cherry Hill, NJ
Sep 19-22, 1995	Los Angeles, CA

CLASSIFICATION MANAGEMENT IN THE NISP 5220.6

DoDSI, Richmond, VA
Feb 28, 1995
Sep 19, 1995

ADVANCED INDUSTRIAL SECURITY MANAGEMENT 5220.4A

Dates and locations to be announced. For information, call Paul McCray, (804) 279-4759.

INFORMATION SECURITY MANAGEMENT 5220.7

Dec 5-16, 1994	Richmond, VA
Mar 27-Apr 7, 1995	Richmond, VA
Jun 5-16, 1995	Richmond, VA
Jul 17-28, 1995	Washington, DC
Sep 18-29, 1995	Richmond, VA

INFORMATION SECURITY ORIENTATION 5220.7A

Oct 12-14, 1994	Newport, RI
Oct 18-20, 1994	Jefferson City, MO
Oct 18-20, 1994	Ft Knox, KY
~~Oct 25-27, 1994~~	~~DLA, Alexandria, VA~~
~~Nov 1-3, 1994~~	~~Mare Island, CA~~
Nov 8-10, 1994	Wright-Patterson AFB, OH
Nov 29-Dec 1, 1994	Arnold AFB, TN
Nov 30-Dec 2, 1994	Public Works Center, HI
Dec 5-7, 1994	Public Works Center, HI
~~Jan 18-20, 1995~~	~~Keyport, WA~~
Jan 24-26, 1995	Pt Mugu, CA
~~Feb 7-9, 1995~~	~~Phoenix, AZ~~
Feb 14-16, 1995	Panama City, FL
Mar 1-3, 1995	DLA, Dallas, TX
Mar 7-9, 1995	Patuxent River, MD
Mar 14-16, 1995	Robbins AFB, GA
Mar 15-17, 1995	Offutt AFB, NE
~~Mar 21-23, 1995~~	~~USAF Academy, CO~~
Apr 4-6, 1995	DIA, Washington, DC
Apr 5-7, 1995	Hurlburt Field, FL
Apr 19-21, 1995	Savannah, GA
Apr 25-27, 1995	DLA, Atlanta, GA
May 3-5, 1995	DLA, Orlando, FL
May 9-11, 1995	Eglin AFB, FL
~~May 16-18, 1995~~	~~New Cumberland, PA~~
Aug 15-17, 1995	Keyport, WA
Aug 30-Sep 1, 1995	DIA, Washington, DC

DoD SECURITY SPECIALIST 5220.9

DoDSI, Richmond, VA
Jan 30-Feb 17, 1995
Mar 6-24, 1995
May 8-26, 1995
Aug 7-25, 1995

AIS SECURITY PROCEDURES FOR INDUSTRY 5220.10

Mar 20-23, 1995	Los Angeles, CA
Mar 28-31, 1995	Secaucus, NJ
Apr 4-7, 1995	Dallas, TX
May 2-5, 1995	Atlanta, GA
May 9-12, 1995	San Francisco, CA
Jul 18-21, 1995	Huntsville, AL
Aug 1-4, 1995	TBD (Midwest Region)
Sep 12-15, 1995	Cherry Hill, NJ

Registration and point-of-contact made through the DIS Regional Office sponsoring the course.

DoD PERSONNEL SECURITY ADJUDICATIONS 5220.11

Oct 17-28, 1994	Richmond, VA
~~Jan 23-Feb 3, 1995~~	~~Ft Meade, MD~~
May 1-12, 1995	Richmond, VA
Jul 17-28, 1995	Richmond, VA

To host this course at your location, call (804) 279-4440, DSN 695-4440.

DoD ADVANCED PERSONNEL SECURITY ADJUDICATIONS 5220.12

~~Feb 27-Mar 10, 1995~~	~~TBD~~
Jun 5-16, 1995	Richmond, VA
Sep 11-22, 1995	Richmond, VA

To host this course at your location, call (804) 279-4440.

TRAIN-THE-TRAINER SECURITY BRIEFERS (TTT/SBC) 5220.13A 5220.13

DoDSI, Richmond, VA

Train-the-Trainer	**Security Briefers Course**
Mar 6-10, 1995	Mar 8-10, 1995
Jun 19-23, 1995	Jun 21-23, 1995
Sep 25-29, 1995	Sep 27-29, 1995

To host the TTT/SBC, call (804) 279-6076.

SECURITY FOR SPECIAL PROGRAMS 5220.14

By invitation only. Call (804) 279-5169, DSN 695-5169 for details.

PERSONNEL SECURITY INTERVIEWS 5220.15

DoDSI, Richmond, VA
~~Dec 6-8, 1994~~
Jul 11-13, 1995

CLASSIFICATION MANAGEMENT 5220.17

DoDSI, Richmond, VA
Jan 9-13, 1995
Apr 24-28, 1995
Sep 11-15, 1995

PERSONNEL SECURITY MANAGEMENT 5220.18

DoDSI, Richmond, VA
~~Nov 14-18, 1994~~
Jan 9-12, 1995
Aug 14-17, 1995

*Feb 28-Mar 3, 1995
*Mar 21-24, 1995
*Apr 4-6, 1995
*Jun 26-29, 1995
*Aug 8-10, 1995
*Oct 3-6, 1995

*Above courses have been changed to on-site classes sponsored by various installations/activities.

To host this course at your location, call (804) 279-4440, DSN 695-4440.

STRATEGIES FOR SECURITY EDUCATION 5220.20

DoDSI, Richmond, VA
Nov 14-18, 1994
Jan 23-27, 1995
Jul 10-14, 1995
Aug 28-Sep 1, 1995

INFORMATION SYSTEMS SECURITY BASICS 5220.22

DoDSI, Richmond, VA
Nov 14-18, 1994
Dec 12-16, 1994
Jan 23-27, 1995
Apr 10-14, 1995
May 15-19, 1995
~~Jun 12-16, 1995~~
Jul 10-14, 1995
Aug 14-18, 1995
Sep 25-29, 1995

By invitation only. Nominations are validated through Information Systems Security program managers at component or agency level. Call (804) 279-6076, DSN 695-6076 for course details.

INTERNATIONAL PGMS SECURITY REQUIREMENTS 5220.23

DoDSI, Richmond, VA
Nov 28-Dec 2, 1994
Feb 27-Mar 3, 1995
May 1-5, 1995
Jul 31-Aug 4, 1995

ESPIONAGE: THEN AND NOW 5220.25

DoDSI / ITC, Fort Washington, MD
Apr 11-14, 1995
Jun 20-23, 1995
Sep 26-29, 1995

American Society
for Industrial Security
Presents this

Distinguished Achievement Award

to

U.S. Department of
Defense Security Institute
Richmond, Virginia

IN RECOGNITION OF

First Place
1993 Video Competition - U.S. Government
"You Can Make A Difference"

PRESIDENT

August 24, 1993
DATE

Award winning video . . .

An 18-minute video based on interviews of convicted espionage felons, designed to motivate employees and military personnel to support personnel security programs through timely intervention.

You Can Make a Difference

This video counters the various anxieties and empowers otherwise loyal and committed employees to get involved with the personnel security process, by adding the emotional impact of having the very people who have destroyed their careers -- the convicted offenders themselves -- tell us they wish someone had been concerned enough to have stopped *them.*

Marked For Official Use Only, it is not releasable for public viewing or to the media. Now being distributed to Federal agencies and departments, cleared contractors may obtain a copy by written request through FilmComm Inc.

To government contractors: Because this is an FOUO product, we ask you to certify in your order that, when received, "This video product will be used only for the training and education of employees or personnel in support of a federal government security program."

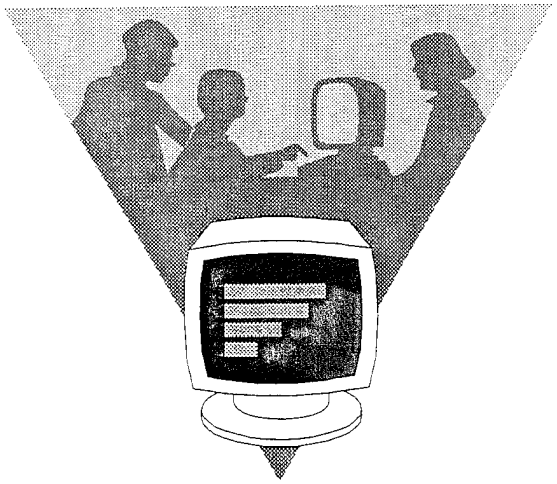
Prepaid cost is $21.50 plus $2.50 for shipping for 1/2".
Invoiced requests are $23.50 and $2.50 for shipping.

} *(For 3/4" add $10.00.)*

For additional ordering details, please call FilmComm.

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

update . . .



AIS Security Procedures For Industry Course (AIS-I)

The 3 1/2 day AIS-I provides contractors with practical experience in reviewing AIS Standard Practice Procedures (AIS SPPs) and conducting AIS Self-Inspections. The Defense Industrial Security Program requirements for processing classified information in data processing and office automation systems are explained, together with supporting rationale.

Topical areas include: discussion of AIS security procedures and guidelines; and applicable AIS SPP outlines prepared and distributed by DIS activities. Using guidance provided during the course, students will review an AIS SPP for a microcomputer system and inspect the system in accordance with Chapter 8 requirements of the Industrial Security Manual (ISM).

There is no tuition for the course and a security clearance is not required. To be eligible for attendance, students must prepare or have oversight responsibility of AIS Approval and AIS SPPs. Upon acceptance to the course, students must complete a series of Work-Ahead-Modules (WAMs) which will be issued to them approximately one month prior to the commencement of the course. Class size is limited, so registration is accomplished on a first come, first served basis.

For additional information, call the Systems Protection Training Team, (804) 279-6076.

Dates and locations:

May 2-5, 1995	Atlanta, GA
May 9-12, 1995	San Francisco, CA
Jul 18-21, 1995	Huntsville, AL
Aug 1-4, 1995	TBD (Midwest Region)
Sep 12-15, 1995	Cherry Hill, NJ

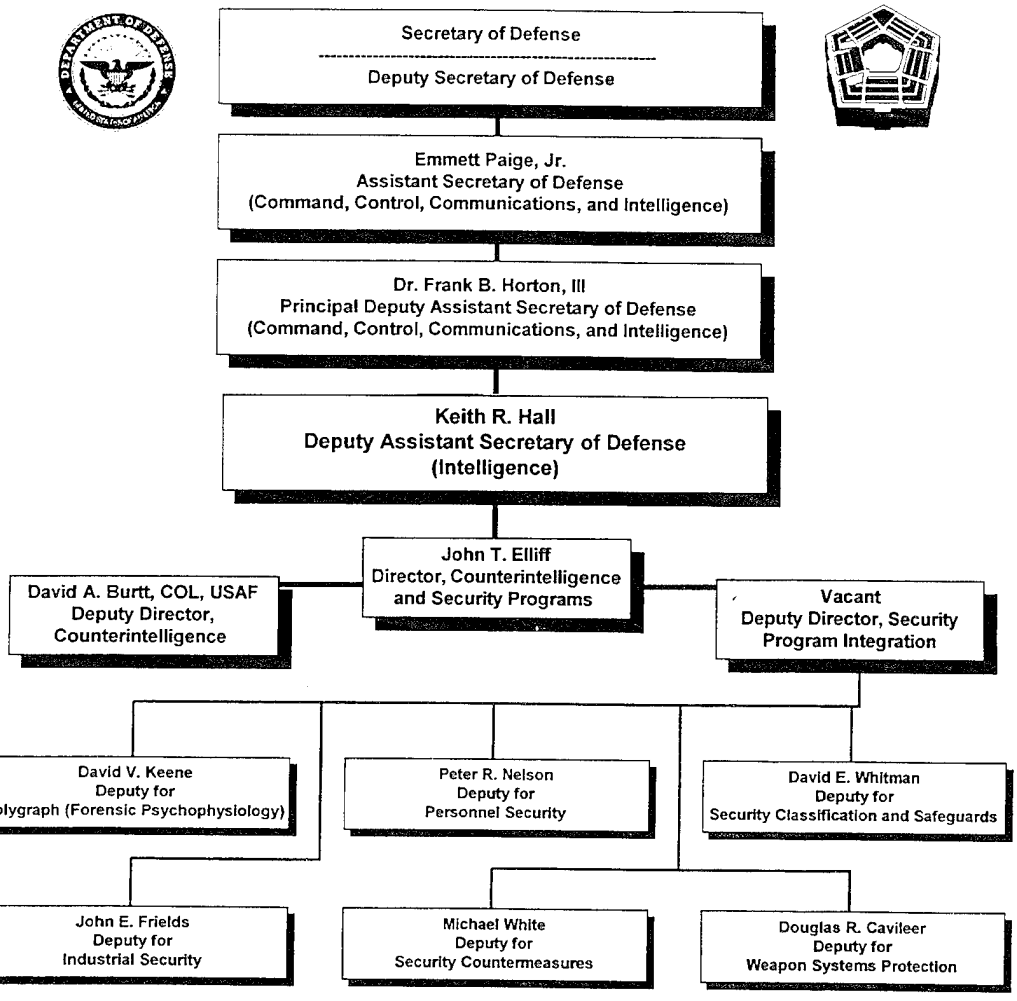
To register, contact the Education and Training Specialist in your DIS RegionalOffice:

Northeast Sector, Boston, MA. Debbie DeMarco, (617) 451-4918
Mid-Atlantic Sector, Cherry Hill, NJ. Lee Greenberg, (609) 482-6509 x 230.
Southwest Sector, Irving, TX. Susan Harrison, (214) 717-0888.
Pacific Region, Long Beach, CA. Linda Kimbler, (310) 595-7666.
Capital Area, Alexandria, VA. Penny Henry, (703) 325-9634.
Southeast Region, Smyrna, GA. Nancy Rosenberger, (404) 432-0826.
Midwest Sector, Chicago, IL. Toni DelVecchio, (312) 886-7737.

OSD in Transition.....

The first two months of this year have been a period of significant change in the offices of the Secretary of Defense which are responsible for defense security and counterintelligence programs. These changes involve both organizational structure and personalities—several of whom have left a lasting mark on our thinking and practice. Since the new year we have bid farewell to Maynard Anderson, Acting Deputy Under Secretary of Defense for Policy; John S. Hoover, Deputy Director for Analysis in the Information Systems Security Directorate; Ray W. Pollari, Director, Counterintelligence; and John G. Grimes, Deputy Assistant Secretary of Defense (CI & SCM)

These retirements have coincided with a restructuring of the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) in those areas having to do with counterintelligence and security. A new organizational chart which follows shows the new position designations and incumbents above and below the office of the Deputy Assistant Secretary of Defense (Intelligence). While most Defense security programs remain under this structure, information systems security and Tempest programs have been moved to the DASD for Command, Control and Communications. It is important to note that in this new arrangement, security and counterintelligence remain closely integrated and are now under a single director. Special Access Programs and International Security will remain with the Under Secretary of Defense (Policy).



Introducing Keith R. Hall

Deputy Assistant Secretary of Defense (Intelligence)

Prior to his appointment as DASD(I), Mr. Hall was Deputy Staff Director for the Senate Select Committee on Intelligence, having primary responsibility for supporting committee members in the annual budget authorization process involving all U.S. intelligence activities. He also played a key role in other committee activities including oversight of intelligence programs, interaction with other Congressional and Executive Branch elements, and review of intelligence related legislation.

Mr. Hall has been involved in U.S. intelligence in various capacities since 1970. He served nine years in Army intelligence where he was assigned to various SIGINT and HUMINT positions, to include two tours where he commanded overseas operational intelligence units. In 1979, having been selected as a Presidential Management Intern, he resigned from the Army and was appointed to the Office of Management and Budget. At OMB he was assigned as the budget examiner for the Central Intelligence Agency, serving in that capacity until he joined the Senate staff in 1983.

Mr. Hall received his BA in History and Political Science from Alfred University, and a Masters in Public Administration from Clark University. He is the recipient of a number of military awards and decorations as well as the OMB Director's Award for Professional Achievement.

Acquisition Systems Protection
Training tools available from DoDSI

Exportable Training Modules

A series of modules on acquisition systems protection for use by presenters at the component, installation, activity, or program level.

- Introduction to Acquisition Systems Protection: *A 90-minute course of instruction designed to orient personnel on the basics of acquisition systems management and introduce the fundamentals of the protection program.*
- Acquisition Systems Protection (Advanced): A 4-hour lesson designed for practitioners developing program protection plans.
- Acquisition Systems Protection for Acquisition Professionals: A 90-minute lesson focusing on the enabling disciplines for protection planning such as security countermeasures, counterintelligence support, operations security, and intelligence support.

Two exportable training modules on system security engineering (SSE) for dissemination to both government and industry. A 90-minute lesson providing an introduction to SSE designed for the acquisition professional. Included are briefer's notes, graphics, training tips, and the ASP Resource Listing.

- Basic overview of Systems Security Engineering
- Training guide for the reissuance of the MIL-STD 1785

Videos

Executive Overview is designed to assist you in introducing the Acquisition Systems Protection Program (ASPP) to your organization. It's primarily a motivational tool to encourage acceptance of the concepts of the ASPP and ensure the program is understood and integrated into acquisition efforts. Produced in May, 1993, the video is 14-minutes long. Designed for government use, but released to contractors supporting defense acquisition efforts is authorized. The video is marked with distribution statement D. Local reproduction is encouraged. This video is a good introduction to the first three exportable training lessons listed above.

Protection Planning focuses on compliance with protection requirements and is an expansion of the Executive Overview video. Approximately 24 minutes in length, the video is designed for Department of Defense employees. It is distributed to government offices and agencies, with release to Defense contractors on request. Local reproduction is encouraged.

Independent Study Course

Acquisition Systems Protection Program DS 6100

This course introduces the general concepts and principles of the Acquisition Systems Protection Program. It will help students develop an understanding of how serious the loss of essential program information is for our national security. The four lessons provide individual learning objectives and self-graded interactive exercises. Included are the protection provisions of DoD Directive 5000.1, Defense Acquisitions; and DoD Instruction 5000.2, Defense Acquisition Management Policies and Procedures. Course covers background of the ASP, the need for program protection, structure and general responsibilities for the ASP program, and an introduction to the Program Protection Plan. To register: submit an Army DA Form 145 to the Army Institute for Professional Development, U.S. Army Training Support Center, Newport News, Virginia 23628-9989.

More Training Materials

Protection Planning Instructor's Guide: A tutorial on program protection that uses a notional program to emphasize the role of various acquisition specialties. Combined with the Protection Planning video, the estimated time for completion is 90 minutes.

Security Awareness Bulletin, April 1993, 1-93. "Acquisition Systems Protection." Edition dedicated to the ASPP, including questions and answers about the ASPP with Dr. John T. Elliff, Director, Defense Security Programs.

To obtain copies of these materials, call (804) 279-6076/5169, DSN 695-6076/5169.

Security Awareness Publications Available from the Institute

Publications are free. Just check the titles you want and send this form to us with your address label

Our address is:

DoD Security Institute
Attn: SEAT
8000 Jefferson Davis Hwy, Bldg 33E
Richmond, VA 23297-5091
(804) 279-5314 or DSN 695-5314

- ❑ **Recent Espionage Cases: Summaries and Sources**. July 1994. Eighty-five cases, 1975 through 1994. "Thumb-nail" summaries and open-source citations.
- ❑ **DELIVER!** Easy-to-follow pamphlet on how to transmit and transport your classified materials. Written specifically for the Department of Defense employee.
- ❑ **Terminator VIII**. Requirements for destruction of classified materials. Contains questions and answer for some common problems and also detailed information on various destruction methods. Written specifically for the Department of Defense employee.
- ❑ **STU-III Handbook for Industry**. To assist FSOs of cleared defense contractors who require the STU-III, Type 1 unit. Covers step-by-step what you need to know and do to make the STU-III a valuable addition to your facility's operations.
- ❑ **Survival Handbook**. The basic security procedures necessary for keeping you out of trouble. Written specifically for the Department of Defense employee.
- ❑ **Layman's Guide to Security**. The basic security procedures that you should be aware of when handling classified materials in your work environment.
- ❑ **Acronyms and Abbreviations**. Twelve pages of security-related acronyms and abbreviations and basic security forms.

Security Awareness Bulletin. A quarterly publication of current security countermeasures and counterintelligence developments, training aids, and education articles. Back issues available from the Institute:

- ❑ The Case of Randy Miles Jeffries **(2-90)** Jan 90
- ❑ Beyond Compliance - Achieving Excellence in Industrial Security **(3-90)** Apr 90
- ❑ Foreign Intelligence Threat for the 1990s **(4-90)** Aug 90
- ❑ Regional Cooperation for Security Education **(1-91)** Jan 91
- ❑ AIS Security **(2-91)** Sep 91
- ❑ Economic Espionage **(1-92)** Oct 91
- ❑ Self-Inspection Handbook **(2-92)** Feb 92
- ❑ OPSEC **(3-92)** Mar 92
- ❑ What is the Threat and the New Strategy? **(4-92)** Sep 92
- ❑ Acquisition Systems Protection **(1-93)** Apr 93
- ❑ Treaty Inspections and Security **(2-93)** Jul 93
- ❑ Research on Espionage **(1-94)** Mar 94
- ❑ Information Systems Security **(2-94)** Aug 94
- ❑ Acquisition Systems Protection Program **(3-94)** Oct 94

For the Record.....

Order any of the following published proceedings from past security conferences and symposiums by sending us a pre-addressed **mailing label** and a note stating which of these publications you would like for your agency or unit reference library.

Proceedings of the 1993 DOD Security Conference (FOUO)

This recently issued volume has been distributed to all attendees; however, it may be of considerable interest to security professionals who were unable to attend the meetings last May. As a guide to policy trends and security issues in the Department of Defense, this publication would be a valuable item in each major command and principal security office.

Proceedings of the JIGSAG International and Threat Symposium August 1992

A few copies remain of the proceedings of this symposium which was organized by the Joint Industry Government Security Awareness Group and held at the Department of Defense Security Institute. Speakers addressed the dramatic geopolitical shifts which directly impact on our concept of the foreign intelligence threat to government and industry. This still-timely information makes interesting reading.

Security Awareness in the 1990s: A Symposium December 1990

Due to continuing demand we have reprinted the proceedings to this conference on the future of security awareness which was held in Monterey, California in December 1990. Many of the presentations made to this one-time symposium on education and awareness are still timely and offer innovative ideas for the security professional.