PERSEREC

PERS-TR-98-001
February 1998

FOREIGN INTELLIGENCE THREAT AWARENESS PROGRAMS:

A REVIEW

prepared for the
National Counterintelligence
Policy Board

DISTRIBUTION STATEMENT A
Approved for public release;
Distribution Unlimited

19980512 038

DTIC QUALITY INSPECTED 1

Defense Personnel Security Research Center
99 Pacific Street, Building 455-E
Monterey, California 93940-2481

FOREIGN INTELLIGENCE THREAT AWARENESS PROGRAMS: A REVIEW

prepared for the

NATIONAL COUNTERINTELLIGENCE POLICY BOARD

February 1998

DEFENSE PERSONNEL SECURITY RESEARCH CENTER
99 Pacific Street, Building 455-E
Monterey, CA 93940-2491

DTIC QUALITY INSPECTED 3

NACIPB

NATIONAL COUNTERINTELLIGENCE POLICY BOARD

WASHINGTON, DC 20505

NACIPB-001-98
6 February 1998

MEMORANDUM FOR: National Counterintelligence Policy Board
National Counterintelligence Operations Board
National Counterintelligence Analytic Working Group
Counterintelligence Training Working Group
Awareness Working Group

FROM: John F. Lewis, Jr.
Chairman
National Counterintelligence Policy Board

SUBJECT: PERSEREC Report, *Foreign Intelligence Threat Awareness Programs: A Review*

1. In March 1996, the National Counterintelligence Policy Board (NACIPB) agreed on the need to review the effectiveness of the US Intelligence Community's foreign intelligence threat training and awareness programs. The Defense Personnel Security Research Center (PERSEREC) was subsequently commissioned to undertake the review with the following objectives:

a. Describe and evaluate the effectiveness of foreign intelligence threat awareness programs in government and industry.

b. Determine the adequacy of programs that train awareness instructors and presenters.

SUBJECT: PERSEREC Report, *Foreign Intelligence Threat Awareness Programs: A Review*

c. Assist policymakers to enrich foreign intelligence threat awareness programs.

d. Recommend improvements where necessary.

2. At the 2 October 1997 meeting, NACIPB members discussed the report's findings and subsequently concurred with its recommendations. On behalf of the NACIPB, I am transmitting, for your information, the completed PERSEREC report entitled, *Foreign Intelligence Threat Awareness Programs: A Review*. While the findings of the report are generally favorable, a continuing obligation exists on the part of all organizations that produce CI information to ensure that our foreign intelligence threat awareness programs remain relevant and proactive.

3. I encourage addressees to review the report's recommendations and initiate early enhancement actions within your respective agencies and departments. As part of its CY 1998 agenda, the NACIPB will schedule a follow-up review of the sufficiency of community actions to implement study recommendations.

John F. Lewis, Jr.
Chairman

Attachment

DEFENSE PERSONNEL SECURITY RESEARCH CENTER (PERSEREC)

99 PACIFIC STREET, BUILDING 455, SUITE E
MONTEREY CALIFORNIA 93940-2481
(408) 656-2448/DSN: 878-2448

December, 1997

Mr. John F. Lewis, Jr.
Chair
National Counterintelligence Policy Board
c/o National Counterintelligence Center
Washington, DC 20505

Dear Mr. Lewis:

In September 1996, as you know, the NACIPB approved a plan developed by PERSEREC to review the effectiveness of foreign intelligence threat awareness programs in the Executive Branch. We developed the plan in response to a request from your predecessor, Nora Slatkin. The attached draft report describes in detail how we conducted the review and presents our conclusions and recommendations. Our method, conclusions and recommendations are outlined briefly below:

We studied 31 Executive Branch agencies and tapped into a variety of sources of information within each agency. We talked with senior policymakers responsible for threat awareness, and interviewed briefers (in the report referred to as providers). We surveyed agency audience members after they had been briefed and facilitated several focus groups. We also conducted independent observations of briefings in the field, and we arranged for a team of counterintelligence experts to review sample awareness materials, such as videos, brochures, etc., to evaluate their effectiveness. In industry, 60 senior representatives were interviewed, mostly directors of security, from companies contracted to the federal government at all levels from unclassified to collateral to SAP/SAR.

On the whole, foreign intelligence threat awareness programs in the Executive Branch and among government contractors are working well. The variability we found in complexity and quality of programs among the agencies is not surprising, given the diversity of the agencies' different missions and the varying backgrounds and talents of the individuals given responsibility for the training. Overall, briefings and instructional materials are adequate or better. Suitable subject areas, or topics, are covered quite well; objectives that counterintelligence experts feel are appropriate for briefings are being largely achieved; presentations are generally well received by audiences; and the briefing content is up to date. Some high-quality instructional materials are available.

Providers consistently indicated their need for interesting, relevant and timely threat awareness information that can be readily adapted for use in their briefings and instructional materials. They also desire speedy and convenient access to current threat data. To improve the quality of threat information, we recommend that the counterintelligence community devote more attention to the selection and preparation of information to be shared with providers. Counterintelligence information-producing agencies should begin to think of FITA providers as part of their overall customer base, clients who constantly need information. To this end, producers should work with their clients to identify the types of information they need and the format they prefer. It may be necessary to *create* materials that are appropriate by sanitizing raw information to design products where just the lessons learned are highlighted and can be shared at the unclassified level.

To make FITA information more accessible, information must be organized to facilitate retrieval and dissemination. Materials are needed where information is organized and cross-referenced in such a way that facilitates access by FITA providers. Information, once organized, should then be made accessible to providers. The counterintelligence community has a number of distribution vehicles, such as INTELINK or INTELINK CI, the U.S. Government Extranet for the Security Professional (ESP), and the Defense Counterintelligence Information System (DCIIS), as well as web sites at DIS, DODSI, DOE and NACIC. Through such vehicles, current classified and unclassified threat information can be made available to providers for the development and preparation of briefings.

We also suggest that the principal counterintelligence agencies provide guidance, additional training, and enhanced supporting products for foreign intelligence threat awareness programs in government and industry. This could be achieved through three vehicles: "how-to" guidance for deciding what information to include in presentations; an unclassified catalog of threat awareness products and where to find them, and a catalog of high-quality sample instructional materials in a CD format. We recommend a series of new videos, centrally produced for economy of scale, that address specific issues (e.g., insider threat, technical threats, etc.), perhaps with segments focused on specific audiences. These should be professionally produced and updated every 2 years.

On behalf of PERSEREC, I would like to thank you for affording us the opportunity to conduct this review. We hope that you will find our report useful and that it may lead to changes that indeed improve foreign intelligence threat awareness programs in the Executive Branch.

Sincerely,

James A. Riedel, Ph.D.
Director

ACKNOWLEDGMENTS

The Defense Personnel Security Research Center (PERSEREC) owes a huge debt to many individuals who have helped us with this study.

Members of the National Counterintelligence Policy Board first conceived of the study and agreed to support it. Staff at the National Counterintelligence Center, in particular Michael Waguespack, Director, and Frank Rafalko, liaison between the Center and PERSEREC, were especially supportive in the process of developing the study terms of reference. We wish also to acknowledge the contribution of Barbara Campbell and Mary Griggs.

The points of contact in the various government agencies in the study willingly agreed to be our guides into their agencies. They gave a great deal of time: describing their programs, helping us develop sampling plans for their agencies, putting us in touch with the right people, answering questions, and reviewing drafts. They acted as real partners in this study and we could not have managed without them.

The many providers who generously allowed us to observe their briefings, responded to a lengthy questionnaire about their jobs as briefers, and spent so much time in personal interviews telling us about their work. Their cooperation, patience and frankness are much appreciated.

Hundreds of audience members--the receivers of briefings--took time to fill out evaluation forms after each briefing. Their additional written comments on the forms were so useful for our understanding of their view of how information gets imparted.

Members of the focus groups gave up a large segment of time to help us grasp in more depth issues related to the effectiveness of foreign intelligence threat awareness briefings.

Representatives of contractor companies participated in lengthy telephone interviews concerning industry's view of awareness programs. Their willingness to speak so openly about issues of importance to industry was most refreshing. We promised them anonymity so we do not list their names, but we are grateful for their contributions.

Lastly, I would like to especially thank the following people: Suzanne Wood at PERSEREC; Marty Wiskoff and Susan Hodgins, our contractors at BDM, International; and Joanne Marshall-Mies and Drew Sands, our subcontractors. These individuals have worked extremely hard on this project for the past year. Our three consultants, Richards Heuer, Tony Palumbo and Chuck Torpy, contributed on several tasks. These ranged from helping us conceptualize and define appropriate foreign intelligence threat awareness objectives and topics, to reviewing text, to evaluating materials. Thanks are also due to Lynn Fischer of the Department of Defense Security Institute who, along with the consultants, introduced clarity into our early thinking. Lynn Fischer produced the paper, *Foreign Intelligence Threat and Security Awareness Topics*, which appears as Appendix C-3 in this report.

James A. Riedel, Ph.D.
Director
PERSEREC

February 1998

EXECUTIVE SUMMARY

Tasking and Objectives

In April 1996, the National Counterintelligence Policy Board (NACIPB) tasked the Defense Personnel Security Research Center (PERSEREC) to review the effectiveness of foreign intelligence threat awareness (FITA)[1] programs in the Executive Branch and among government contractors. The National Counterintelligence Center (NACIC), as Executive Secretariat of the National Counterintelligence Policy Board (NACIPB), was appointed as project manager. Work on the review began in August 1996, and the study plan, prepared by PERSEREC, was approved by the NACIPB in September 1996.

The objectives of the review were to (a) describe FITA activities in the Executive Branch and evaluate their effectiveness; (b) determine briefers' (referred to in this study as *providers*) perceptions of their capacity to effectively prepare and present briefings, and their views on organizational factors that may inhibit their ability to deliver effective briefings; (c) provide policymakers with information to help enrich programs by highlighting examples of excellent FITA materials; and (d) recommend improvements in the FITA system throughout government and industry.

Approach and Methodology

With the aid of counterintelligence consultants, we developed a list of FITA learning objectives, along with a list of topic areas that should be addressed in any FITA program. An example of a learning objective is that by the end of the briefing the audience will know how to recognize indicators of possible foreign intelligence interest or activity. An example of a topic is the types of information being targeted. These two lists--learning objectives and topics--were used frequently in the study as benchmarks for evaluating the effectiveness of FITA activities. We examined the programs of the 31 Executive Branch agencies or organizations identified for us by NACIC[2] , by using five different sources of information. These sources were (a) senior-level points of contact (POCs), to acquire an overall perspective and to discuss policy; (b) providers who conduct briefings, for their nuts-and-bolts knowledge of the FITA world; (c) audiences, the recipients of the briefings, for their responses to briefings, including five focus

---

[1] FITA is a study-devised acronym for *foreign intelligence threat awareness* which we use throughout this report simply for ease of reading. Apologies to the counterintelligence community for inventing yet another government acronym.

[2] In a few cases, we did not go further than initial interviews with the points of contact. For example, the NSC, a policy advisory board, does not have its own developed FITA program; foreign travel and other threat awareness briefings are provided by other agencies, such as the FBI, on request.

groups who discussed briefings in depth; (d) observations of briefings in the field to see if objectives were met and the topics were up to date; and (e) materials used to disseminate the message (e.g., videos, briefings, brochures, handouts, etc.).

The agencies varied greatly according to size and mission. Some agencies are major FITA information providers, others receive information. Our methodology--tapping five sources of data--allowed us the possibility of sampling at different places in any agency, whatever the size or mission. In total we received protocols from 71 providers, surveys from 1,401 audience members, and made 61 briefing observations.

We also interviewed 60 senior representatives, mostly directors of security of companies contracted to the federal government, at all levels from unclassified to collateral to SAP/SAR.

Findings

Counterintelligence and Threat Awareness Authority and Policy

Our review of the policy guidance documents pertaining to FITA requirements reveals that the documents have largely been updated in light of the end of the Cold War. In the few instances where documents are outdated, plans are under way to revise them. For the most part the policies clearly state the objectives and requirements for FITA programs.

Counterintelligence and Threat Awareness Programs in the Executive Branch

The agencies under review vary widely in size and mission and, consequently, in the way they deliver threat information and whether counterintelligence is integrated within the security program or conducted separately. The major counterintelligence agencies also differ somewhat in their formal roles and missions. These counterintelligence agencies brief generally at three different levels (their own counterintelligence people in pure counterintelligence briefings, and their employees and their contractors in threat awareness) and they produce threat awareness products for dissemination to themselves and others. Some smaller agencies' programs are serviced by larger agencies in terms of both briefings and awareness products.

Providers of FITA Information

Providers' primary responsibilities are in security or counterintelligence. Paygrades for civilian providers range from GS-11 to 15, with most being GS-12s and 13s. For the military, ranks vary from E4 up to 0-3, with most being junior officers or senior enlisted. On the average, providers have spent about 10 years in FITA-related fields, and for most people FITA is a part-time activity. The majority receive their training while on the job, although many have taken some basic courses in presentation skills.

Very few providers have their presentations routinely measured by agency audience surveys, but for the most part they believe they are doing a good job, especially in their speaking abilities, their credibility and their mastery of the subject. Our audience surveys present a strong

endorsement of these providers and the quality of their information: 74% gave ratings of excellent or above average. Our observers who attended briefings rated them just slightly lower (72% excellent or above average). Our observers rated more briefings below average or poor than did the audiences.

FITA Briefings

Providers present FITA information in a variety of briefings: initial security, security refresher, foreign travel, anti-terrorism, nontraditional threat, and other special presentations. Briefings are typically given to groups of 25 or more. Travel briefing audiences are usually much smaller, frequently fewer than 10 people. The majority of briefings are conducted at the unclassified level and usually consist of a standup lecture, often with viewgraphs, 35mm slides, or computer-based visuals. Handouts are often used to augment the presentation. Briefings are given to all cleared employees and to people of all ranks. Individual agency policies decree how often briefings are given; some agencies, however, conduct briefings on an as-needed basis or, in the field, when they can be scheduled around other demands.

Most providers would prefer, if policy allows, to rely on briefings they develop themselves. But certain agencies insist on providers using standardized briefings produced at headquarters so that the major message is standardized. Several providers mentioned they inherited their briefing materials from predecessors. Almost all say they make some attempt to tailor briefings. The majority get information for briefings from other parts of their own organization and from the National Counterintelligence Center (NACIC), Central Intelligence Agency (CIA), the Department of Defense Security Institute (DoDSI), and the Federal Bureau of Investigation (FBI), plus other counterintelligence agencies. The two organizations receiving the highest rating by providers for quality were NACIC and DoDSI. As for making materials readily available to other agencies, top ratings were given to the Department of Energy (DOE), NACIC and DoDSI. Additional sources of information are security publications, databases, newspaper articles and, to a lesser extent, security seminars.

FITA Objectives

On the whole, the objectives used as FITA benchmarks in this study are being achieved in most agencies. Our audiences give high marks for most. For example, audiences almost always learned how to recognize indicators of possible foreign intelligence interest or activity. On the other hand, the data suggest that some providers are not doing as well in presenting the kind of message that deglamorizes espionage and makes it clear that those who do commit espionage will be caught and punished. Nor are providers doing well in clearly defining how people's own behavior, especially while in foreign countries, may unintentionally attract foreign intelligence interest.

The Currency of the FITA Message

During the study, our researchers found the message to be up to date. At no time did they encounter currently used general briefing content where the message was out of date or reflected

old Cold War concepts. Occasionally, old espionage cases were used, but only to illustrate issues that had timeless validity. Providers are eager to acquire up-to-date information having to do with present-day issues, such as "new" methods used by both traditional adversaries and current allies, computer hacking, etc. Nontraditional threat and economic espionage are the most salient FITA items.

Materials

Currently used, FITA-related materials examined by our experts contained no outdated references to the Cold War. An effort has been made to bring all products in line with current realities. Our experts, however, while agreeing there was a great deal of useful and good information in the products, feel that many products did not do a good job of integrating the information. The message is not always pulled together adequately or is left to the inductive abilities of the audience, e.g., there may be an excellent portrayal of the threat, but no advice given on how to get employees to recognize indicators and how to report them. Many of these materials lack well-stated objectives; a specific statement of the threat (foreign intelligence or insider); clear instructions on what the audience should look for; how and when to report suspicious activity (with an explanation of *why* they should report); and an appealing, modern style and format. On the other hand, several excellent examples of FITA materials were found in use.

Organizational Support

Providers stress the importance of having upper-management recognize that there is still a serious threat and thus give more support to FITA programs. They want to see managers involved with the program and personally attending. They believe if management is interested and committed, it will allocate the increased resources required for developing materials and also make more time available to cover the subject adequately.

Interagency Communication

Many people complained of a lack of FITA-supporting communication among the counterintelligence agencies and recommended more interagency contact at a formal level. At the same time, providers find their own way of obtaining information. They network with colleagues, their "links" in other agencies, for information they need.

Industry

Industry representatives explained that their main sources of FITA information were the FBI, NACIC and Defense Investigative Service (DIS). Like its government counterparts, industry finds less formal ways to acquire information, such as through professional associations, commercial threat analysis services, and personal contacts within government. The topics covered in industry briefings reflect a slightly different set of priorities than in the government briefings in that they tend to emphasize personnel security indicators, vulnerabilities during foreign travel, sources of the threat, modus operandi of foreign agents, and insider threat and volunteer spies.

The primary requirement from industry is relevant and current threat information. While generic information is adequate, most companies would prefer regional-, industry-, company- and technology-specific information. There is a general belief that government is holding back on threat and counterintelligence information, although for the most part industry recognizes that not all helpful information can be shared. A second major theme in industry, as companies look towards international markets, is the problem of protecting not just classified but proprietary information. Industry wants up-to-date, country-specific threat information so that their employees, exposed to potential problems when working with business partners from other countries, can be informed.

Conclusions and Recommendations

Conclusions

FITA programs in the Executive Branch and among government contractors are generally effective. For the most part, briefings and instructional materials are adequate or better. Some variability is not surprising given the diversity of agencies' missions, and the number of individuals with varying backgrounds and inevitably different degrees of talent who have responsibility for FITA training. Overall, we found the requisite topics were covered quite well in FITA presentations, the briefing objectives achieved, the presentations well received by audiences, and some high-quality instructional materials available.

More specifically, we conclude that:

1. **Presentation content is up to date and reflects the post-Cold War climate. But greater emphasis is needed on the issues of insider threat and personnel security indicators.** In recent history, most espionage has been conducted by insiders who volunteer their services to a foreign intelligence service. The information revolution, post-Cold War openness, global economic competition, new and nontraditional intelligence adversaries, and certain other social and economic trends all combine to create an even more fertile ground for volunteer espionage. Audiences should learn this fact and must be taught to spot characteristics in a person that indicate he or she might be a security risk.

2. **A significant obstacle to fully effective FITA programs is a lack of access to current information on a number of topics.** Providers in both government and industry report a need for current information concerning not just traditional threats, but the nontraditional threat, economic espionage, computer hacking, etc. They want more detail about what technologies are being targeted, and how and by whom. And they seek a centrally monitored place to obtain such information: a database or a homepage where they can find relevant and current threat information, classified or otherwise.

3. **Objectives used as benchmarks in this study are largely being achieved with one notable exception--discouraging and deterring individuals from committing espionage.** We believe that more emphasis on this objective is required. The message should deglamorize

espionage and focus on the high probability of detection and the adverse personal impact of betrayal on the offender, family and friends.

4. **Presentations, for the most part, are well received by most audiences.** Despite negative reactions to FITA from some "unwilling customers" who believe that there are no longer foreign intelligence threats, most people endorse the providers and the credibility of the information provided. While most providers say they are adequately prepared for their responsibilities, more than half indicated a need for more training in presentation techniques. Also some are eager to improve their presentations with modern instructional aids and materials; to get away from the "crooked viewgraph" technology.

5. **On the whole, instructional materials provide good content**. However, the content is sometimes lost in an inadequate and only partially presented message. Guidance is needed to help providers develop their own materials. Improved means for disseminating high-quality instructional materials also are needed.

6. **More detailed and current case study information is required**. It is not necessary to reiterate a spy's entire life history in a briefing; rather, specific information from cases, old and new, can be extracted to illustrate certain points that a provider would want to make, such as a spy's motivations, reporting suspicious behavior, or explaining the sad consequences of espionage, for the nation or offender. People relate to case histories more easily than to general statements. Old cases can certainly help to teach these lessons, still relevant today. Newer cases, of course, may be fascinating to audiences, but will have little instructional value unless they are related to specific learning objectives.

7. **In some cases in an organization coordination between counterintelligence and security functions is good and in others, where these functions are separated, less effective**. Given that betrayal by insiders is a principal threat, the distinction between threat awareness and security awareness virtually disappears; this makes essential the close coordination between counterintelligence and security professionals for exchange of information and planning of FITA activities.

8. **Management emphasis on, and support for, FITA is uneven**. In some agencies, managers are personally involved in FITA activities and provide the resources required for developing good materials and allocating the time to cover material adequately. NSA's re-awareness program is a possible model for some agencies to follow. It integrates re-awareness training into the security clearance (periodic reinvestigation) process and demonstrates management support for the program. Managers in some agencies, however, sometimes take the threat less seriously and thus tend not to provide adequate support for the program. Some even are said to treat FITA as a check-the-box requirement. Such an attitude means that fewer resources are allocated to FITA programs. And this cavalier approach trickles down the system to the rank-and-file who in turn may learn not to take FITA and reporting responsibilities seriously.

Recommendations

1. **Improve the quality and accessibility of threat information**. Providers consistently indicated their need for interesting, relevant and timely threat awareness information that can be readily adapted for use in their briefings and instructional materials. They also desire speedy and convenient access to current threat data. Availability of these data through automated networks would facilitate widespread access for providers and afford a more rapid and consistent portrayal of the foreign intelligence threat throughout government and industry.

(a) *To improve the quality of threat information for use by FITA providers, the counterintelligence community needs to devote more attention to the selection and preparation of information to be shared with providers.*

Getting threat awareness information to providers should be an essential part of the counterintelligence mission; and counterintelligence information-producing agencies should begin to think of FITA providers as part of their overall customer base, clients who constantly need information. To this end, producers should work with their clients to identify the types of information they need and the format they prefer. It may be necessary to *create* materials that are appropriate by sanitizing raw information to design products where just the lessons learned are highlighted and can be shared at the unclassified level.

(b) *To make FITA information more accessible, information must be organized to facilitate retrieval and dissemination.*

Some existing data sources offer good information, but are not formated for easy retrieval. For example, in newsletters information is organized by publication date and not generally indexed by subject. Materials are needed where information is organized and cross-referenced in such a way that facilitates access by FITA providers.

Information, once organized, should then be made accessible to providers. The counterintelligence community has a number of distribution vehicles, such as INTELINK or INTELINK CI, the U.S. Government Extranet for the Security Professional (ESP), and the Defense Counterintelligence Information System (DCIIS), as well as web sites at DIS, DODSI, DOE and NACIC. Through such vehicles, current classified and unclassified threat information can be made available to providers for the development and preparation of briefings.

2. **Principal counterintelligence agencies should provide guidance, additional training, and enhanced supporting products for FITA programs in government and industry.**

Supporting products and services would include the following:

(a) *"How to" guidance for deciding what information to include in presentations and instructional materials.* This guidance would assist providers in making their presentations more relevant to the jobs of audience members, a need expressed by observers and audiences alike. Recommended scripts, generic briefing slides or "suggested formats" should be developed to assist providers in developing their own presentations and materials. Specific guidance concerning what information to present will help providers decide on the topics that are most appropriate for their situation and particular audience.

(b) *A FITA resource catalog* in an unclassified format that describes products and briefing support resources (videos, briefing packages, CBT modules, recurring publications, web sites, and points of contact) specially for FITA, along with specific information about how to obtain all products.

Providers were found to be only moderately prepared to locate resources needed to develop or deliver threat information. Some lack the experience required to know where to find FITA resource materials and services. For others, conducting presentations is a collateral duty and they are unfamiliar with the sources of FITA products and services. Providers need to know how to request products and services pertaining to FITA. They also need more information about sources for training opportunities.

It is recommended that NACIC be the lead agency to prepare and circulate this briefing resource catalog. A start has already been made with NACIC's products catalog (classified), DoDSI's Announcement of Products and Resources for the security educator, and PERSEREC's new version of the Desktop Resource Guide.

(c) *Sample instructional materials.* While instructional materials may provide some good content, the point is often lost in an inadequate or partially presented message. Twenty-five to 50% of providers report that they are not well prepared to design effective presentations and instructional aids. They also say they lack state-of-the-art technology to make their presentations dynamic and to create really good instructional materials. Providers need guidance for preparing their own instructional materials. A catalog of high-quality sample materials in a CD format should be developed for easy adaption. This would increase the quality of instructional materials throughout the counterintelligence, security and intelligence communities. Time and money could be saved because providers would not have to develop materials from scratch.

3. **Develop a series of FITA videos**

More videos and short video clips need to be created, each addressing a critical theme or topic. The FITA source catalog recommended above would make more accessible the good videos already available. While videos are not as personal as a briefing and cannot be tailored perfectly for a particular audience, they can be a very useful instructional aid in combination with other media such as briefings or printed materials. Videos provide a means to consistently communicate the foreign intelligence threat in a high-quality manner. They are especially useful for smaller organizations that do not develop their own FITA materials. However, they do need to be updated regularly and frequently to maintain their relevance.

4. **Foster greater management support for FITA**

Some providers of FITA information report that lack of management support is undermining their ability to achieve FITA objectives. This problem becomes manifested in inadequate resources, the low priority given to FITA relative to other organizational programs and functions, only perfunctory involvement in FITA activities by managers, and an unwillingness by managers to publicly acknowledge the reality and seriousness of the threat. Lack of support erodes the credibility of the providers of FITA information and may result in some managers sending a message symbolically that the foreign intelligence threat is neither a real nor serious problem--a direct contradiction of the message that providers are attempting to communicate.

Managers need to take steps to increase support in terms of adequate financial resources, sufficient staff and time for FITA activities, and improved oversight. They should become personally involved in FITA activities to demonstrate their importance and help correct the perception by some that there no longer is a foreign intelligence threat now that the Cold War is over. They should assure institutional commitment by having all employees under their cognizance participate in and support FITA activities. Managers need to assure good coordination between counterintelligence and security functions to foster an appropriate exchange of information and planning of FITA activities. Finally, managers should develop measures of effectiveness for FITA activities and evaluate them accordingly.

5. **Provide training for FITA providers**

More training opportunities should be made available to providers. Some providers indicated that they need more training, either in developing the content of presentations or in presentation techniques, or both. The evaluation of the instructional materials revealed that good content is often lost in an inadequate and only partially presented message. There is a need to better prepare FITA providers to develop printed materials, design effective audiovisual aids, bring routine material alive and design effective presentations. Many providers also would like exposure to courses specifically addressing various counterintelligence topics and types of threat information.

Suggested agencies to develop this training are either NACIC or DoDSI. DoDSI's current course, *Strategies for Security Education*, could be reinvented to address FITA training needs.

TABLE OF CONTENTS

ACKNOWLEDGMENTS i

EXECUTIVE SUMMARY iii

TASKING AND OBJECTIVES iii
APPROACH AND METHODOLOGY iii
FINDINGS iv
CONCLUSIONS AND RECOMMENDATIONS vii

TABLE OF CONTENTS xiii

LIST OF TABLES xvi

INTRODUCTION 1

TASKING 1
OBJECTIVES 1
APPROACH 2
- Project Team 2
- Framework for Evaluating FITA Effectiveness 2
- Procedures for Collecting Information 3
- Sources of Information and Methods of Collection (Government Agencies) 3
- Collection and Evaluation of Materials 5
- Sources of Information and Methods of Collection (Industry) 5

CAVEATS 6

FINDINGS 7

COUNTERINTELLIGENCE AND THREAT AWARENESS AUTHORITY AND POLICY 7
COUNTERINTELLIGENCE AND THREAT AWARENESS PROGRAMS IN IHE EXECUTIVE BRANCH: A BRIEF OVERVIEW 9
PROVIDERS AND THEIR BRIEFINGS 11
- Experience and Involvement with FITA 11
- Types of Audiences, Briefings, and Printed Materials 11
- Developing Briefings and Sources of Information 13
- Methods of Presenting Threat Awareness Information 14

SUBJECT-MATTER EXPERTISE, PRESENTATION SKILLS, AND TRAINING OF PROVIDERS 15
TOPICS COVERED IN FITA BRIEFINGS 16
- Sources of the Threat 18
- Modus Operandi of Foreign Intelligence Agents and Services, and Collectors 18
- Technical and Non-HUMINT Threat 19
- Foreign Travel Vulnerabilities 20
- Types of Information Being Targeted 20
- The Threat and Security Countermeasures 21
- Consequences of Espionage for the Offender and the Nation 21
- Insider Threat and Volunteer Spies 22
- Personnel Security Indicators and Vulnerabilities 23

USE OF ESPIONAGE CASE STUDIES 23
IMPEDIMENTS TO EFFECTIVE COMMUNICATION OF THREAT INFORMATION 24
- Post-Cold War Climate 24
- Emphasis on Threat Awareness 24
- Access to Threat Information 25

Providers' Qualities and Skills 26
Instructional Resources 26
EFFECTIVENESS OF THE FITA MESSAGE 26
Audience Evaluations 27
Briefing Observations 32
Materials Evaluation 34
Examples of Excellent Materials 37
THE VIEW FROM INDUSTRY 39
Types of Audiences 40
Types of Briefings and Printed Material 40
Development of Briefings and Materials 41
Briefing Topics 42
Subject-matter Expertise and Presentation Skills 44
Overall Assessment 44

CONCLUSIONS AND RECOMMENDATIONS 46

APPENDICES

APPENDIX A GLOSSARY OF ACRONYMS A-1

APPENDIX B PROJECT TEAM B-1

APPENDIX C FOREIGN INTELLIGENCE THREAT AWARENESS
C-1 Foreign Intelligence Threat Awareness Learning Objectives C-1
C-2 Foreign Intelligence Threat Awareness Topic Areas C-3
C-3 Foreign Intelligence Threat and Security Awareness Topics C-7

APPENDIX D PARTICIPANTS
D-1 Participating Agencies D-1
D-2 Participating Companies D-3

APPENDIX E COUNTERINTELLIGENCE AND THREAT AWARENESS AUTHORITY AND POLICY E-1

APPENDIX F AGENCY DESCRIPTIONS
F-1 Air Force Office of Special Investigations (AFOSI) F-1
F-2 Army 902d Military Intelligence Group F-3
F-3 Central Intelligence Agency (CIA) F-7
F-4 Coast Guard (USCG) F-11
F-5 Department of Commerce (DOC) F-15
F-6 Customs Service F-19
F-7 Defense Information Systems Agency (DISA) F-23
F-8 Defense Intelligence Agency (DIA) F-27
F-9 Defense Investigative Service (DIS) F-31
F-10 Department of Defense Security Institute (DODSI) F-35
F-11 Department of Energy (DOE) F-39
F-12 Federal Bureau of Investigation (FBI) F-43
F-13 Federal Emergency Management Agency (FEMA) F-47
F-14 Joint Staff (JS) F-49
F-15 Department of Justice (DOJ) F-51
F-16 Marine Corps (USMC) F-55
F-17 National Aeronautics and Space Administration (NASA) F-57
F-18 National Counterintelligence Center (NACIC) F-61
F-19 National Imagery and Mapping Agency (NIMA) F-63
F-20 National Reconnaissance Office (NRO) F-67
F-21 National Security Agency (NSA) F-69
F-22 Naval Criminal Investigative Service (NCIS) F-73

F-23 Nuclear Regulatory Commission (NRC) F-77
F-24 Office of the Secretary of Defense (OSD) F-81
F-25 On Site Inspection Agency (OSIA) F-83
F-26 Security Policy Board (SPB Or Board) F-85
F-27 Senate F-87
F-28 Department of State (DS) F-89
F-29 Department of Treasury (DOT) F-93

APPENDIX G DATA COLLECTION INSTRUMENTS
G-1 Questions for Interviewer Guidance for Agency Point of Contact Interviews G-1
G-2 Foreign Intelligence Threat Information Providers Interview Protocol G-3
G-3 Audience Survey G-15
G-4 Focus Group Protocol G-17
G-5 Briefing Observation Form G-23
G-6 Sample Materials Evaluation Form G-29
G-7 Industry Providers of Foreign Intelligence Threat Information Telephone Protocol G-31
G-8 Topic Evaluation Form for Industry Representatives G-33

LIST OF TABLES

TABLE 1 Classification Levels of Different Types of Briefings 12
TABLE 2 Preparedness for Various Tasks 15
TABLE 3 Topics Covered as Reported by Providers and Observers 17
TABLE 4 Surveys by Type of Briefing 27
TABLE 5 Rating of Briefings by Audiences 28
TABLE 6 Focus Group Agreement That Goals Were Met 30
TABLE 7 Size of Briefing Audience 32
TABLE 8 Type of Briefing 32
TABLE 9 Observers' Assessment of Emphasis Placed on Various Learning Objectives 33
TABLE 10 Observers' Ratings of Presentations 34
TABLE 11 Percentage of Respondents Who Report Briefing Various Types of Personnel 40
TABLE 12 Method of Disseminating FITA Information 40
TABLE 13 Sources of FITA Information for Industry 41
TABLE 14 Topics in Industry FITA Briefings 43

INTRODUCTION

Tasking

In March 1996, at a meeting of the National Counterintelligence Policy Board (NACIPB),[1] questions were raised regarding the effectiveness of foreign intelligence threat awareness programs. From this discussion a tasking developed in April 1996 from NACIPB to PERSEREC. This tasking requested PERSEREC to review the effectiveness of foreign intelligence threat awareness (FITA)[2] programs in the Executive Branch and among government contractors. NACIC, as Executive Secretariat of the NACIPB, was appointed as project manager. Work on the review began in August 1996, and the study plan, prepared by PERSEREC, was approved by the NACIPB in September 1996.

Objectives

The objectives for the study were developed collaboratively between PERSEREC researchers and the NACIC staff, with input from the Security Policy Board staff.

(a) Describe FITA programs and evaluate their effectiveness

This objective involved (1) assessing the degree to which FITA information is current, accurate and relevant and reflects post-Cold War realities, and (2) assessing the attitudes and perceptions of FITA briefing audiences about the briefings they receive.

(b) Determine briefers' (referred to in this study as *providers*) perceptions of their capacity to function as effective briefers

This objective focused on determining (1) the extent to which providers of FITA information believe that they have the knowledge, skills and abilities or subject-matter expertise required to prepare and present effective briefings, and (2) agency-specific organizational conditions that inhibit the effectiveness of FITA efforts.

---

[1]From this point on in the report we refer to all agencies and organizations by their acronyms. For these and other common abbreviations, please see the glossary of acronyms in Appendix A.

[2] FITA is the study-devised acronym for *foreign intelligence threat awareness* which we use throughout this report simply for ease of reading.

(c) Provide policymakers with information to enrich programs in the future

This objective involved (1) collecting examples of excellent materials that could be highlighted and used as possible models by other agencies, and (2) reviewing FITA programs with an eye toward making recommendations for improvements in the FITA system.

Approach

Project Team

A nine-person project team[3] was established consisting of (a) six researchers to plan the project, collect and analyze data, and interpret and present results; and (b) three counterintelligence experts, retired from AFOSI, CIA, and FBI, to provide consulting assistance throughout the effort.

Framework for Evaluating FITA Effectiveness

Our first task was to review in depth the whole domain of FITA. Under what authority and policies are FITA activities conducted and what is the general structure of FITA programs in the Executive Branch? In addition, what is the purpose of FITA activities? What topics should be covered? What should audiences take away from them? Such detailed information would give us benchmarks or standards against which to measure presentations and other FITA activities in the field. With the aid of our consultants, we assembled a list of appropriate learning objectives for FITA[4], along with a list of topic areas that are consistent with the objective of delivering relevant, current and accurate threat information to employee populations.[5] These two lists were vetted with selected counterintelligence experts in the field. In addition, Appendix C-3[6] discusses further the topics, provides rationale for their selection, and gives a number of quality indicators that might serve as a basis for evaluating prepared briefings, publications and other communications.

An example of a learning objective is that by the end of the presentation the audience will know how to recognize indicators of possible foreign intelligence interest or activity or will understand their obligation to report suspicious or improper activity to appropriate authorities. An example of a topic that is important to address in FITA presentations is a discussion of the sources of the threat (with examples of countries involved in intelligence operations against the U.S., case examples of allied countries involved in intelligence operations against U.S. interests, and examples of threats to U.S. information from nonstate entities such as terrorist groups.)

---

[3] Appendix B
[4] Appendix C-1
[5] Appendix C-2
[6] Appendix C-3

It is recommended that the reader review these lists (in Appendix C-1 and C-2) before continuing to read this report, because these lists are used frequently in questionnaires in the study as benchmarks for evaluating the effectiveness of FITA activities.

Procedures for Collecting Information

Thirty-one government agencies[7, 8] (and points of contact [POCs]) to be included in the review were identified by NACIC. These agencies[9] ranged from major intelligence agencies to smaller agencies without well-developed FITA programs. With the help of these agency POCs, procedures were established for collecting information. Within each agency a sampling plan was developed to identify appropriate FITA providers and how best to reach them, set up a system for gathering sample materials, and determine where and when to conduct briefing observations, audience surveys and focus groups.

Sources of Information and Methods of Collection (Government Agencies)

To thoroughly examine FITA activities from as many perspectives as possible, we used five different sources of information. These sources were agency POCs, providers of FITA information, audiences' responses to briefings (including five focus groups), observations of briefings, and FITA materials. For each of these sources, we designed different methods for acquiring and recording the data. Some agencies, due to the limited nature of their FITA programs, were unable to provide extensive information, and our data-collection was sometimes limited to interviews with a POC and perhaps a single provider. We devoted the majority of our resources to the study of agencies with larger FITA programs.

The sources and corresponding methodologies used to elicit information are briefly described below. For detailed information on procedures used for each source, please refer to the sections covering these sources that appear later in the report.

---

[7] Appendix D-1

[8] NACIC identified 31 agencies or organizations. In a few cases, we did not go further than initial interviews with the POCs. For example, the NSC, a policy advisory board, does not have its own developed FITA program. Foreign travel and other threat awareness briefings are provided to it by other agencies, such as the FBI, on request.

[9] Not all the entities we studied are literally federal agencies. For example, the Security Policy Board is a board, the NSC a council, etc. But for purposes of convenience, we use the word *agency* when referring to them.

Interview of Agency Points of Contact

In order to acquire an understanding how FITA information is disseminated within an agency, we interviewed POCs in each agency.[10] In addition to providing us with an overview of the agency's FITA program and the policies under which it operates, the POC helped develop a sampling plan for the research in that agency, identified appropriate providers in the best position to help us, and acted as liaison and facilitator between our researchers and the agency. The 31 POC interviews were conducted in the greater Washington, DC area.

Interview and Survey of FITA Information Providers

Other invaluable sources of information were the providers themselves, those individuals who actually conduct FITA briefings and participate in other FITA activities. These individuals are a major part of the process of getting FITA information to the audience. Thus, we interviewed them and also administered a lengthy questionnaire[11] to capture their perceptions from their level in the organization of how the system works. We asked providers to describe their experience with FITA: how they prepare briefings, what topics they cover, their training, and their opinions on what could be done to improve the system in their agency. Most provider interviews were conducted in the greater Washington, DC area. We planned to conduct between 3 and 6 provider interviews in each agency; in some cases we conducted more than 6, in others none.

Survey of Audiences' Response to Briefings

An additional viewpoint was obtained through information acquired from the recipients of briefings, the audience. What do they think about the briefings? What do they know after a briefing? What have they learned to do when they observe suspicious behavior? What do they think about the material covered and the individual who was conducting the briefing? To acquire this information, we administered a survey[12] to audience members after a briefing. We attempted to conduct between 1 and 5 audience surveys per agency, but in some agencies we obtained none. Audiences ranged in size from a single person to 150. Again, most of these surveys took place in the greater Washington, DC area, but others were administered at briefings in other locations.

---

[10] Appendix G-1
[11] Appendix G-2
[12] Appendix G-3

Focus Groups with Recipients of Briefings

Another way of measuring audience response to briefings was focus groups--structured, small-group interviews in which we acquired rich, indepth information on audiences' reactions.[13] Asking people to spend an hour or two discussing a briefing in detail gave us a different insight into what makes a good FITA briefing and what captures and holds an audience's attention. Five focus groups were conducted.

Observation of Briefings in the Field

Briefings are the core of the FITA program in an agency. Thus, our researchers attempted to assess the extent to which the contents of these briefings were current and relevant to audiences, met certain learning objectives, and covered appropriate topics in a manner that reflects current realities. Between 1 and 3 briefings per agency were observed and a briefing observation form[14] was used to record observers' responses. Many of the briefings were conducted in the greater Washington, DC area. However, other briefings were observed in Albuquerque, NM; Draper, UT; Fort Benning, GA; Fort Leonard Wood, MO; Livermore, CA; Los Angeles, CA; Oakland, CA; San Diego, CA; Sunnyvale, CA; Travis Air Force Base, CA; and Vandenburg Air Force Base, CA.

Collection and Evaluation of Materials

Materials include all the ways of disseminating FITA information to audiences. Videos, briefings, brochures and pamphlets, newsletters and handouts are examples of some of the materials used. To ensure that the basic message is current and up to date, we conducted an evaluation of a sample of these materials using a panel of counterintelligence and security experts.[15]

Sources of Information and Methods of Collection (Industry)

We had also been tasked by the NACIPB to explore industry's participation in FITA activities. Because of the large numbers of contractor companies, we elected to interview a sample of representatives on the telephone.

Appropriate POCs in facilities supporting government programs[16] were selected by key officials from contractor associations--NCMS, AIA and CSSWG. We used these professional associations as *entree* because they could identify facilities in private industry who have need for FITA information and who deal with a whole range of programs, from proprietary to collateral to SAP/SAR. The facilities selected represented a

---

[13] Appendix G-4
[14] Appendix G-5
[15] Appendix G-6
[16] Appendix D-2

wide variety of different missions and government customers. We sent invitations to 173 facilities, received 80 responses expressing willingness to participate in the study, and actually interviewed 60 individuals. Interviews[17] were designed to elicit how foreign intelligence threat information is disseminated at each facility. We were interested in the scope of the program, the types of audiences being briefed, the methods and media used by providers, and the providers' sources for FITA information. We also wanted to know what problems were felt to exist, and how the POC thought those problems might be solved. In addition to the telephone interviews, POCs filled out a checklist[18] of topics covered in their facilities' FITA activities.

Caveats

In studying 31 Executive Branch agencies, it was impractical to interview every counterintelligence expert in each organization, observe every counterintelligence briefing, or watch every counterintelligence video. We requested agencies to select briefings and providers that would best represent the agency and this may have introduced a slight bias. We believe that overall we have captured the essence of each agency's program, including the program structure, what briefings are like, what providers feel about their work and training, and what audiences think about briefings. We also attempted to apportion our effort so that the agencies with the most significant FITA programs received the greatest attention.

In industry, we established a sampling plan to include a wide range of facilities--from those addressing highly sensitive SAP/SAR programs to those primarily concerned with company proprietary information. While our sample of facilities is not representative of all industry, it does encompass the types of companies and programs that need to be sensitive to FITA concerns.

This study focuses primarily on the review of FITA activities in the Executive Branch and in industry. It was not designed to explore full counterintelligence programs. Counterintelligence is a big umbrella of which FITA is but one spoke.

One last point. The word *effectiveness* is used throughout this study. Since the ultimate criterion of a program cannot truly be measured--whether any sensitive information was protected or any would-be spies were deterred as a direct result of any FITA briefing--we looked at the process, the program in place. We looked at people's opinions about whether the correct message is being sent, whether it is heard and internalized, and whether the audience ultimately understands how to behave under certain circumstances (i.e., report certain types of activity). We asked providers how they perceive their own ability to get the message across and how successful they think they are; we asked observers to rate briefings objectively; and we asked audiences how they feel about a given briefing. Through this multifaceted approach, we believe we obtained a balanced view of FITA activities.

---

[17] Appendix G-7
[18] Appendix G-8

FINDINGS

We begin the Findings section with a discussion of counterintelligence and threat awareness authority and policy, followed by a brief overview of counterintelligence and threat awareness programs in the Executive Branch. We then turn to discussions of providers and their briefings; providers' subject-matter expertise, presentations skills and training; topics covered in FITA briefings; use of espionage case studies; impediments to effective communication; effectiveness of the FITA message; and the view from industry.

Counterintelligence And Threat Awareness Authority And Policy

We examined Executive Branch guiding policies affecting counterintelligence and FITA programs. (See Appendix E for a description of many of these policies.) Our main purpose was to determine the degree to which responsibilities and objectives are clearly outlined and policies are current and relevant to modern-day realities. Another purpose was to try to understand how closely policy is followed at headquarters and in the field.

All policy documents are implemented by executive departments using directives and regulations that are tailored to fit the special needs of the agency. In addition, depending on the size of the department and its perceived vulnerability to foreign intelligence targeting, subordinate agencies and components usually further implement their departmental directives to fit particular subordinate requirements. Consequently, large departments, such as DoD, have significant numbers of cascading policies that affect programs down to the lowest major operating level. By contrast, many smaller departments may have no subordinate implementing directives.

E.O. 12333 *U.S. Intelligence Activities*, December 4, 1981, is the major policy guidance for intelligence and counterintelligence. It assigns roles and responsibilities for collecting foreign intelligence information and for conducting counterintelligence programs. The fact that it is dated 1981 seems scarcely to matter, given the broad nature of its contents and taskings.

Another overarching policy--and one more directly relevant to our study of FITA programs--is PDD/NSC-12 *Security Awareness and Reporting for Foreign Contacts*, August 5, 1993. This document requires that each department or agency in the U.S. government maintain a formal security and/or counterintelligence awareness program. Such a program should ensure a high level of employee awareness of the threat; provide for the reporting of employee contacts with foreign nationals in which unauthorized access to information is sought; and be tailored to meet the particular needs of the agency. All this must be done while ensuring that employees' privacy and freedom of association are protected. Again, this guidance is implemented at the departmental level through a series of directives, instructions and regulations.

Other related executive orders include the recent E.O. 12958 *Classified National Security Information*, April 20, 1995, and E.O. 12968 *Access to Classified Information*, August 4, 1995, also implemented at the departmental level. These orders, on different subjects, are related to FITA because they are supportive of sound awareness programs.

The points of contact in the various Executive Branch agencies whom we interviewed for this study were, of course, very familiar with these policies. However, the actual work of promoting FITA in the Executive Branch is conducted in compliance with implementing layers of directives, regulations and instructions. For example, DoD Directive 5240.6 *Counterintelligence Awareness and Briefing Program*, July 16, 1996, is the fundamental, workhorse directive for the DoD and related counterintelligence programs. Recently updated, this directive lays out requirements for all DoD employees to report information on individuals or events that could pose a threat to U.S. personnel, DoD resources, or classified national security information. The directive requires that each DoD component establish a program to keep employees aware of the threat, teach them how to identify reportable situations, and inform them of their responsibilities to report suspicious situations.

A related directive, DoD Directive 5240.2 DoD *Counterintelligence*, June 6, 1983, has long been recognized as dated and is, in fact, presently being reissued in order to update policy and responsibility for DoD components engaged in counterintelligence activities. Also, the DoD's major directive on terrorism, DoD-0-2000.12 *Combatting Terrorism Program*, September 16, 1996, was recently re-written in light of the Khobar Tower terrorist incident in Saudi Arabia, and is currently being revised once again. The directive tasks commanders and managers with ensuring that the threat from terrorism be understood by DoD personnel and their families, and that individuals understand the procedures that are in place for their protection and safety.

At the next level, each military service writes its own version of DoD policy, based on its own specific needs. The major policy documents for the Army and Air Force concerning FITA were both updated in the early 1990s. Army Regulation 381-12 *Subversion and Espionage Directed Against the U.S. Army*, is dated January 15, 1993 and AF Instruction 171-101, Vol I, Chapter 3, *Counterintelligence and Protective Service Matters,* was issued July 22, 1994. The Navy is presently working on a revision of OPNAVINST 5510.1H, Chapter 5, *Counterintelligence Matters to be Reported to the Naval Investigative Service*, which has not been changed since 1988.

Other defense agencies, such as DIA, DIS, Joint Staff, On-site Inspection Agency, NRO and NSA, and non-DoD agencies, such as CIA, Commerce, Customs and FBI, etc., also have their own regulations, details of which are described in Appendix E.

Several POCs at agency headquarters (both DoD and non-DoD) indicated that, although policy is in place for the local level, headquarters has relatively little control over how and when these various policies are implemented in the field. In the field, local commanders or managers are supposed to see that FITA programs are carried out in a

required manner and on a proper schedule. The impression gathered by our researchers is that in the field briefings are sometimes subject to the exigencies of the job and are scheduled on an ad hoc basis.

To summarize, most policy guidance related to FITA in the Executive Branch appears successfully to address FITA objectives, and is up to date and responsive to the post-Cold War environment. Where policy guidance is occasionally out of date, it is being revised.

Counterintelligence And Threat Awareness Programs In The Executive Branch: A Brief Overview

Counterintelligence is defined in E.O. 12333 as "information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including personnel, physical, document or communications security programs." The recently reorganized counterintelligence structure at the national level is headed by the NACIPB which develops and recommends for implementation major counterintelligence policy, goals and planning directives. It also coordinates the development of interagency agreements and is responsible for monitoring coordination of the various national-level counterintelligence programs. Under the NACIPB are various elements, two key ones being the NACOB and the NACIC. The NACOB proposes and coordinates counterintelligence operations among the key counterintelligence operational agencies, in conjunction with the NACIC. The more broadly focused NACIC coordinates policy development, implements interagency counterintelligence activities, and manages some common-concern programs. It also provides selected national-level counterintelligence products and services for the U.S. government and the private sector.

The five major counterintelligence agencies are Air Force OSI, Army MI, CIA, FBI, and NCIS, with other significant players being DIA, DIS, DOE, NSA, and State. These agencies differ from each other in terms of overall mission and, therefore, in their individual execution of counterintelligence responsibilities.

The FBI, a federal law enforcement agency, for example, is also the primary U.S. counterintelligence agency, with internal security responsibility for the U.S. to prevent and stop espionage and terrorism. (The three military counterintelligence agencies also exert considerable, similar effort, but within the military services' jurisdiction, and in coordination with the FBI.)

The CIA has a primary foreign or positive intelligence role, with counterintelligence being important, but secondary, overall. The CIA has no authority to conduct criminal investigations and technically no law enforcement responsibility. Outside the U.S., however, the CIA is responsible for coordinating certain counterintelligence activities and investigations of the Air Force, Army and Navy, very

much like the FBI coordinates inside the U.S. While AFOSI and NCIS are organized similarly to the FBI, Army MI combines counterintelligence and intelligence in the same agency and, like CIA, does not have law enforcement authority.

The State Department conducts certain counterintelligence investigations of Department personnel in coordination with the FBI and others. NSA does not engage in pure counterintelligence activities, but is a producer of vital information that directly supports the various counterintelligence agencies. DIA primarily collects intelligence through its attaches and other means; it also produces counterintelligence products as part of its major intelligence production effort. DOE, and other agencies not having a primary intelligence, counterintelligence or law enforcement role, are important players in the counterintelligence community, but often essentially for their own internal security purposes or as supporters of the main national counterintelligence effort.

Agencies in the federal government are required by PDD/NSC-12 to institute FITA programs in order to educate employees about how to recognize possible espionage and terrorist activities by a foreign intelligence service and what to do in terms of reporting incidents to appropriate authorities in their agency. These programs must include periodic awareness briefs as well as instructive briefings prior to foreign travel.

The 30 Executive Branch agencies in the study (plus the one Legislative Branch participant, the U.S. Senate) present a wide variety of FITA programs, each with its own special counterintelligence awareness mechanisms, depending on each agency's overall mission. Some programs, such as the military services, are extremely large, with literally hundreds, perhaps thousands, of providers. They, and other agencies with highly sensitive missions, like CIA, NSA and NRO, have very complex programs: they brief and educate at three levels (to their own counterintelligence staff, to their own employees in general, and to their contractors); they produce materials; they service smaller agencies; and they service their contractors and, in some cases, train the contractors in awareness program requirements. Agencies at the other end of the spectrum have less developed programs. The NRC, as one example, is a relatively small agency without a formal FITA program per se, and relies on a single person to develop and disseminate threat awareness information for its newcomers and travelers.

Several agencies produce threat materials. Examples of these are the CIA, DIA, DIS, DoDSI, DOE, FBI, NACIC, NRO, NSA, State, and the military service counterintelligence organizations. On the other side, smaller agencies scramble to acquire any pertinent materials they can "beg, borrow or steal" to enrich their programs.

Several agencies are specifically designated to provide counterintelligence services, including awareness programs, to entities outside their normal arena. For example, Air Force supports OSD and the Navy supports the DISA. DIA provides counterintelligence briefing support for the Joint Staff.

Major counterintelligence agencies, such as NCIS and the other military service organizations, centrally manage materials and the types of briefings being given in the field. By contrast, others, such as DOE and NASA, rely heavily on their field programs, granting them full autonomy and discretion over the content of their programs.

The POCs from each of the 31 agencies in the study discussed the scope of their individual programs. Each agency's program is summarized in Appendix F. A reading of these descriptions will reveal the wide diversity of programs among agencies.

Providers and Their Briefings

The providers--those individuals in Executive Branch agencies who actually prepare and conduct FITA briefings--were a major source of information in our study. Seventy-one providers of FITA information representing 22 of the 31 agencies were interviewed. (The other agencies were either policy-writing agencies without briefing programs of their own, or agencies with programs that were extremely small; for these, a single POC interview sufficed to describe the program. In addition, some agencies declined our request for information from providers.) Providers were asked about their personal experience with FITA: the types of audiences they address and the types of briefings they conduct, how they develop their briefings, what topics they cover, and the media they prefer to use.

Experience and Involvement with FITA

Sixty-five percent of the providers described their current, primary responsibility as counterintelligence; 25% stated that they were security officers, 6% identified themselves as law-enforcement professionals, and 4% were in intelligence or other positions. Pay grades of civilian providers ranged from GS-11 to 15, with 79% being GS-12s and 13s. Roughly one-third of the providers in our sample were military, with ranks ranging from E-4 to 0-3. Of these military people, 77% were either junior officers or senior enlisted. On the average, respondents had spent about 10 years in FITA-related fields in the course of their careers. FITA was a part-time activity for most people. Only 14% said that they spend more than 80% of their time on FITA. Sixty-three percent spent less than 40%.

Types of Audiences, Briefings, and Printed Materials

In discussing the types of audiences they brief, providers described an entire range of people: from E-1s to the highest officer ranks in the military (including Reserves and National Guard), and civilian DoD employees; from GS-1s to SESs in non-DoD departments; from rank-and-file contractors to chief executive officers of government-contracting companies. Often, because of the type of briefing, all ranks and levels were briefed at the same time. For example, an initial security briefing may include all newcomers regardless of rank. Other times, in travel briefings (at government labs, for example) the audience may be extremely homogeneous, e.g., scientists going abroad to

work together on a particular project. Another example of a homogeneous audience would be foreign service officers' travel briefings before being posted abroad.

Some agencies, such as the FBI, with a special tasking to brief private industry in addition to their own people, brief professional associations; national, state and local civic leaders; and various task forces. NACIC also has a special responsibility for briefing private industry, as does OSAC (State).

We asked the providers the extent to which they emphasize threat information in the various types of briefings. Naturally, all threat awareness briefings emphasized threat information. The next type of briefing most frequently emphasizing threat information was foreign travel. This was followed by security refresher briefings and then, least frequently, initial security indoctrination briefings.

When we looked at the typical size of audiences for the various types of briefings, we found that for the threat awareness, initial security and security refresher briefings about 75% of the time audiences consisted of groups of more than 25 people. For travel briefings the audiences had 10 people or less about 80% of the time.

Concerning the classification levels of different types of briefings, Table 1 shows that between 3-15% of the providers reported conducting threat awareness briefings, initial security briefings, security refresher briefings and foreign travel briefings at both levels--classified and unclassified--depending on the audience and other circumstances. Initial and refresher security briefings are more often than not given at the unclassified level while foreign intelligence threat awareness and foreign travel briefings are as likely to be conducted at the classified level as the unclassified.

TABLE 1
Classification Levels of Different Types of Briefings

	Both Classified and Unclassified %	Unclassified Only %	Classified (All Levels) Only %
Threat awareness	14	43	43
Initial security	3	71	26
Security refresher	10	62	28
Foreign travel	15	42	43

We asked providers who present unclassified briefings if they could be more effective if the briefings were classified. While some agreed, about two-thirds said no, suggesting that they were satisfied that briefing at the unclassified level can be quite effective. We then asked those who brief at the classified level if they could have been

more effective in an unclassified setting. Again, about two-thirds said no, they did not think they could be more effective at the unclassified level.

In summary, providers reported that the classification level at which they are currently briefing audiences is, on the whole, the most appropriate for achieving their objectives for particular audiences.

Developing Briefings and Sources of Information

Central to assessing the effectiveness of a threat message is an understanding of how the message is formulated. Thus, providers were asked how they go about developing their briefings. Do they have learning objectives? Do they design their own briefings or rely on canned materials? If they develop their own briefings, where do they obtain the information? And what do they think about the quality and availability of that information?

Seventy-two percent of the providers said they do have briefing objectives. They are developed by headquarters policy--simply to teach awareness and to explain to people their reporting responsibilities. Objectives are not only set forth in general agency policy but are often scripted into briefings. Objectives may also be delineated in the security manual or presented in canned briefings. Other providers, within the bounds of policy, make up their own objectives; these may fluctuate according to the audience or to a specific region travelers may be visiting. The remaining 28%, who do not develop formal objectives, reported that there is no real necessity for objectives because it is impossible to measure whether objectives have been achieved. However, formal objectives or not, most providers' ultimate goal is simply to get the information across to the audience.

Providers were asked about how they develop their briefings. Do they rely on canned briefings, or develop briefings from scratch themselves? Sixty-eight percent said they rarely use canned briefings. In fact, 74% rely greatly on briefings they develop themselves. And almost all (97%) said that, for the most part, they tailor their briefings to fit particular target audiences. The few who do not attempt to tailor the briefings say that they do not have enough time, there are pressures from headquarters to stay with a centrally developed message, or that the audiences are often so diverse that it is impossible to tailor.

We asked about the sources of information that providers rely on in developing their briefings. Security publications (45%) were the major source, followed by various databases (36%). Newspaper articles (22%) and security seminars (16%) were used less often.

We asked respondents to indicate the most frequently used sources of information for their briefings. They said that most often they acquired their information from within their own organizations. Outside sources most frequently mentioned (in descending order of frequency of use) were NACIC, CIA, DoDSI, and FBI. Also mentioned were DOE,

DIS, NSA, nongovernment security organizations, State and NRO. In terms of quality of these materials, with the exception of one organization, every organization received a rating of average or higher. The two organizations receiving the highest ratings for quality were NACIC and DoDSI. As for ready availability of materials, top ratings were given to DOE, NACIC and DoDSI. There were four organizations that were rated average or below. These lower scores can be explained by the fact that some agencies are, by design, not information-disseminators.

Methods of Presenting Threat Awareness Information

The most common method for delivering threat awareness information is the formal standup briefing to fewer than 50 people. This is followed by briefings in large groups (more than 50), and then by one-on-one or small groups. Much less frequently used are seminars or discussions groups. And computer-based training on LAN or diskette is used even less. Viewgraphs and handouts are the most popular media used in support of presentations. Other less frequently used media are government-produced videos, guest experts, and posters and other visual reminders. Slide shows with audio are infrequently used. Providers also mentioned that they use video segments from news shows/TV specials.

We asked which media providers found most useful and which the least. These are listed below, with their pros and cons.

(a) **Computer presentations, slide shows and viewgraphs**: Computer presentations and slide shows are stimulating to audiences, easy to update and tailor for special audiences, and are portable on laptops. They are better than the old-fashioned viewgraphs which one provider described, with some humor, as often being "dull and always crooked." Besides, they are outmoded technology. On the other hand, others believe that viewgraphs are useful because they can easily be changed to suit an audience; they are easy to use and do not depend on high-tech systems for support.

(b) **Experts**: Audiences like to hear information from the horse's mouth, from people's direct experience. But there are often problems in scheduling guest speakers.

(c) **Handouts/ brochures**: These are cheap to produce and allow for wide dissemination. They are relatively easy to update and serve as reinforcements of the message. People can take them away for future reference. Others report that handouts often get thrown away unread.

(d) **Posters**: If they are produced in-house, posters can reflect the agency's view of security. Others say that it's too costly to produce tailored posters. In any case, while posters are vivid and easy to understand, people quickly get used to them (they are no longer "seen" after a few days).

(e) **Videos/video clips**: These add interest to a briefing by providing examples to which people can relate. Others dislike them because, if they are produced centrally, they cannot be tailored to an agency mission. Videos also lose their currency quickly and, if they have been seen before by an audience, they can be boring.

Subject-matter Expertise, Presentation Skills, and Training of Providers

We asked providers their views on how they would rate their own personal subject-matter expertise and presentation skills, and their views on their past training and desire for future training.

Eighty-six percent described themselves as having sufficient subject-matter expertise to communicate threat information effectively. But they still need current information on counterintelligence activities, computer and technical security issues, and on terrorism.

Regarding presentation skills, as can be seen in Table 2 below, providers gave themselves high marks on most tasks concerned with preparing for and delivering their briefings. Designing audiovisual aids and developing printed materials scored lower, possibly because someone else in the office has this as a primary activity. This could have implications for training, however.

TABLE 2
Preparedness for Various Tasks

	Well Prepared %	Not Well Prepared %
Speak before an audience	87	0
Project professional credibility	84	6
Keep audience's attention	84	0
Find resources needed to develop or deliver threat information	79	8
Be well received by senior-level audiences	78	3
Design effective presentations	77	4
Bring routine material alive	72	9
Design effective audiovisual aids	56	27
Develop printed materials	50	28

Regarding past and future training, we asked how many years it had been since our respondents had received training. Responses were fairly evenly spread, ranging from less than 1 year to more than 7. While training was not always recent, 84% of the individuals we spoke with reported that they had, in fact, received special training to help them make effective presentations. Many reported having received professional or military training as well as a number of specialized courses in topics such as briefing presentation skills and professional development by subject area. Overall, the courses received above-average ratings in terms of quality and value. The training was conceptually sound, well designed and used well-integrated methods and instructional aids. Finally, the providers found the courses relevant to their jobs.

When asked if additional training would help them and, if so, what courses they would like to take, nearly half of the respondents reported that they would indeed like more training, either in content or technique, or both. Many seek current counterintelligence/threat information, and a few want more courses on how to present briefings. Only a handful mentioned specific courses from various agencies.

Topics Covered in FITA Briefings

One of the major taskings from the NACIPB was to assess the degree to which FITA information reflects post-Cold War realities. Therefore, the central focus of the study was to identify the topics that are being addressed and to evaluate the content of the message related to the topics. Examples of such topics are sources of the threat, modus operandi of foreign intelligence services, types of information being targeted, insider threat and volunteer spies, etc.

As explained earlier, we developed a list of topics that cover the domain of FITA information and a set of criteria for evaluating the content of the message related to these topics. The topics and criteria were carefully vetted with counterintelligence professionals to ensure that they indeed covered what one might wish to see in threat awareness briefings appropriate for this day and age. (The reader may wish to refer again to Appendix C-2 for the list of topics and criteria.)

We wanted to gather data that would permit us to draw some conclusions about the extent to which these topics are addressed. However, we knew the 71 providers we interviewed were only a subsample of the whole universe of providers and we wanted another source of information so that we could look at the problem from a different angle. This other source was the observation of some 61 briefings in the field by independent observers. In this way, we hoped to identify some convergence between the two perspectives.

Table 3 compares providers' responses to a question as to whether each of the topics was addressed during the briefings with researchers' observations of whether these topics were actually discussed during briefings.

It should be noted in reviewing Table 3 that the provider percentages reflect a general estimate for *their* total set of briefings, whereas the percentages for briefings observed relate only to those that were viewed by our researchers. The data suggest some degree of congruence between what the providers say they cover and the topics that our researchers observed. The observers generally saw the topics being covered less frequently than the providers' estimates, which is to be expected because researchers only saw a small set of all briefings.

TABLE 3
Topics Covered as Reported by Providers and Observers

Topic	Of 71 Providers Reporting %	Of 61 Briefings Observed %
Sources of the threat	94	90
Modus operandi for FIS	90	90
Technical and non-HUMINT threat	88	69
Vulnerabilities of foreign travel	88	57
Types of information being targeted	87	80
Threat and security countermeasures	85	74
Consequences of espionage for offender & nation	82	59*
Insider threat and volunteer spies	78	62
Personnel security indicators	72	75

*Consequences for the nation was covered in 70% of the briefings observed and consequences for the offender 48%. We averaged these two to produce 59%.

Before discussing in detail the topics that providers actually cover and how well they address them, we present providers' comments on how they initially decide what topics to include. Just as when they develop their objectives, the choice of topic often depends on the organization's mission and the particular needs of the audience--their level of interest, what particular countries they are to visit, currency of the threat, threats to themselves personally or to their agency, threats learned from earlier travelers' experience, etc. Some referred directly to headquarters policy. For example, counterintelligence course materials have often been long established, and providers stick closely to these. Some providers are given (or take) more leeway to use their own judgment in selecting topics. Often this is done through consulting with the audience or with security managers on audience training requirements and interest, simply asking the requester of the briefing, or examining the agency's own classified threat analysis materials.

What follows is a detailed discussion of each of the topics from the perspective of each group. We look at the degree to which *providers* say they are addressing the topics and their perceptions of their adequacy in discussing the topic, and compare this with what the *observers* saw in their briefing observations.

Sources of the Threat

Providers: Ninety-four percent of the providers reported that they address this topic and they have high confidence in their ability to do so. Of these, 85% feel they do a good job. In their open-ended comments they say they emphasize the traditional subject of foreign intelligence services: characteristics and profiles of intelligence collectors, what is being sought, the dangers for employees at home and abroad from intelligence services, etc. They also discuss the fact that, despite the end of the Cold War, a threat still remains. Emphasis is now on discussion of the friendly vs. traditional threat and the dangers of economic espionage by our traditional foes as well as our present allies. Discussions cover which countries are committing economic espionage against the U.S., what technology these countries are seeking, and how they go about getting it. Several stress the dangers to U.S. industry.

Only a few mentioned terrorism and international crime as sources of the threat, but several emphasized the importance of the insider threat, the individual within an agency who makes the first move to contact a foreign intelligence service.

A theme that cuts across most of these responses is the necessity of using concrete examples and detailed case studies to illustrate points. A few providers said they are constrained in what they can say if they are working at the unclassified level.

Observers: In those briefings observed by our researchers, 90% of the providers covered sources of the threat. Most of the time providers do give examples in classified briefings of countries being involved in intelligence operations against U.S. interests. Less frequently they provide case examples of allied countries involved in intelligence operations against U.S. interests, or examples of threats to U.S. information from nonstate entities such as foreign organized crime, terrorist groups, and foreign companies. In fact, only about half the briefings covered these two latter areas.

Modus Operandi of Foreign Intelligence Agents and Services, and Collectors

Providers: While 90% of the providers reported that they cover this topic, only three-quarters of these individuals felt equipped to adequately address it.

They describe in some detail the recruitment cycle: how foreign intelligence agents spot, assess and recruit; characteristics they exploit in their targets, with case examples (e.g., sexual or financial vulnerabilities, greed, revenge, etc.). They discuss trade craft used by both traditional and nontraditional adversaries, specifically recruitment/collection strategies and techniques, such as ethnic targeting and false flag

recruitment; eavesdropping and technical espionage; hotel bugging and bag jobs; electronic interception; unsolicited requests for information; solicitation through telephonic, electronic and personal contacts, etc. Several discuss the problem of volunteer or insider spies and how foreign intelligence services handle volunteers.

Again, many providers stress the importance of using stories and case histories to illustrate real-life events.

Observers: Observers reported that 90% of the briefings include material on modus operandi. Providers frequently describe techniques for eliciting information. They also caution audiences to limit discussions about their work when talking with foreign representatives. Less frequently covered is ethnic targeting, both in terms of defining it and presenting illustrative case material. This issue was covered in less than half the briefings.

Technical and Non-HUMINT Threat

Providers: Eighty-eight percent of providers reported they address this topic and, of these, 84% feel they do a good job. They say that the major subject discussed under this topic is computer security, with examples of how easily hackers can penetrate computers. Another related topic is communications vulnerability: on the Internet, and on open telephones, faxes, cellular phones and electronics. Audiences are urged to use secure devices when transmitting sensitive information and to be alert to general, common-sense OPSEC issues. The problem of technical surveillance is also discussed, including different countries' interception capabilities.

A couple of providers felt that not enough time is spent discussing hackers and computer intrusion cases, and that they lacked information and examples. Also this subject depends on the audience and their level of interest. Providers felt this is a difficult topic because many audiences are not interested in the topic. So providers are tempted to simply not discuss it at all. On the other hand, some agencies' employees are, by the very nature of their work, already deeply versed in this subject and do not always need more information.

Observers: Observers report that in 69% of the briefings they saw the topic of technical and non-HUMINT threat being addressed. Providers frequently discuss foreign intelligence targeting of encrypted voice, fax and data communications. Discussions of the current threat by hackers to restricted information systems and computer networks and reasonable countermeasures to minimize electronic eavesdropping occur fairly often. Less frequently covered is the subject of other non-HUMINT collection methods, such as IMINT, SIGINT, etc.

Foreign Travel Vulnerabilities

Providers: Eighty-eight percent of the providers say they address the topic. Of these individuals, 91% feel that they do a good job. They report in open-ended comments that travel briefings are conducted on a country-specific basis where the special vulnerabilities for the particular country are explained. Providers often specialize in various countries and regions of the world. These briefings almost always contain a general discussion of foreign intelligence service modus operandi: covert monitoring; computer theft; harassment/provocation; dangers at airports, in planes, in hotels and conference rooms; theft or searches of luggage; surveillance, telephone taps, bugs, efforts to elicit information, etc. The discussion then goes on to suggest ways travelers might deflect or neutralize such efforts. Travelers are taught to keep a low profile and what to do if they realize they are being targeted. Several providers try to illustrate their briefings with the use of real-life examples of agency coworkers who have been approached while abroad.

Travel briefings often cover simple personal safety as well as foreign intelligence service methods. And terrorism is frequently discussed in this context, along with how to behave if taken hostage.

Observers: Observers reported that only 57% of all the different types of briefings they saw covered this topic, but that 100% of the pure foreign travel briefings covered it. Providers addressed technical surveillance measures directed at U.S. citizens abroad; examples of covert searches and theft, or compromise of classified or proprietary materials while en route, or at hotels; and general guidelines for the traveler at a foreign location on how to counter any espionage threat. Examples of how U.S. citizens might be targeted, even in allied countries, were given less often.

Types of Information Being Targeted

Providers: Eighty-seven percent of the providers reported they discuss this topic and they have confidence in being able to cover it; 84% of these people feel they do a good job. Depending on the audience, they describe a wide range of types of information: political and economic; military plans, strategies and capabilities; national defense information; signals intelligence and cryptology; all critical leading-edge technologies; trade secrets; company-proprietary, company-sensitive; advanced dual-use technologies; government databases; known targets of one specific foreign service, etc.

For some of the intelligence agencies, the target information is "everything," presumably because in these agencies they work on sensitive information all the time; "everything" is secret and, therefore, a possible target. One person reminded us that targets are not necessarily information alone, but can often be the people who handle the information.

Observers: Observers tell us that 80% of the briefings they saw included material on types of information targeted. Providers did a fairly good job of outlining current interest in dual-use and economically significant technology and of reviewing specific technologies that have been targeted. However, only about half the time are the high-priority targets addressed (e.g., those in the National Security Threat List [NSTL]).

The Threat and Security Countermeasures

Providers: Eighty-five percent of the providers indicated that they cover this topic and, of these, 88% feel that they do a good job in addressing it. They discuss the importance of the employees' role in recognizing a threat when they see it and their obligation to report it to Security. Several make the point that Security cannot do its job without the employees, who are their eyes and ears. The employees are presented as a most important element--they should take an active role in a team effort with the security personnel.

Some providers stress that it is often the employees themselves who are the target. So instruction is given on what to do if they are approached and they are reminded again that any such incident should be reported. The topic of how people should behave to avoid attention, both at home and abroad, is often discussed.

We observed that none of the providers appears to have specifically mentioned that they explain to audiences the reasons behind all the countermeasures such as clearances, gates, barriers, etc., the assumption being that if employees understand the reasons for these countermeasures they will be more willing to comply with the program. Providers' responses emphasized the how, not the why. Perhaps the why is considered too obvious to discuss.

Observers: Observers noted that this topic was covered 74% of the time in the briefings they saw. For these briefings, providers *did* explain the rationale for security countermeasures in terms of specific threat information, and somewhat less frequently showed how lessons learned from specific cases have led to the adoption of security countermeasures.

Consequences of Espionage for the Offender and the Nation

Providers: Providers report that they cover this topic in 82% of the briefings and, of those who do cover it, 93% feel that they cover it adequately. Most providers use case studies to show how espionage leads to a large personal loss for the offender: loss of clearance, job, and freedom, and dire loss for the family. The long jail sentences meted out for spies are stressed. Frequently the subject of consequences for the nation verges on the classified so it is often covered only in general terms. Topics in unclassified briefings include loss of technology; loss of technical advantage; damage to international security, to include political and military interests; and U.S. economic competitiveness and scientific capability. In some of the intelligence agencies, espionage consequences are

given little coverage since employees in those agencies are believed to be already so sensitized to the problem.

Observers: Observers reported that 59% of the briefings they saw covered this topic. Regarding the effects of espionage on the offender, providers use case examples that portray the level of despair and suffering by the people directly or indirectly involved with the espionage and in citing case studies that illustrate the severity of prison sentences in serious cases.

With respect to national consequences of espionage, providers usually address the different types of damage caused by espionage (e.g., loss of life, and damage to intelligence systems, diplomatic negotiating strength, military edge and economic opportunities). They are somewhat less likely to discuss specifics about damage (or potential damage) from recent espionage cases, as might be expected. And they provide little concrete information about damage from classified or other official sanitized sources.

Insider Threat and Volunteer Spies

Providers: Seventy-eight percent cover this topic, but of these only two-thirds feel that they can discuss it adequately. They stress the fact that most U.S. spies are volunteers and, as one intelligence agency provider put it, they can really "burn" their agencies. It is ironic, therefore, that this topic is not covered as frequently as the foreign intelligence threat.

Providers generally discuss such a volunteer's likely motivation. They also try to stress the importance of supervisors and coworkers learning to look for the classic behavioral indicators that might suggest espionage (and they explain what such indicators might be and that any such behavioral anomalies should be reported immediately.) Case studies are widely used, and a few providers say they emphasize the enormous damage caused to the U.S. by these volunteers.

In general, however, going beyond simply saying that most spies are volunteers is difficult because the topic can quickly become very sensitive. Nobody seems to want to create a climate where coworkers are encouraged to mistrust each other or where the government is seen not to trust its own people. Some providers reported that they stress the need to report on coworkers not just to "catch a spy," but as a helpful way of perhaps preventing the budding volunteer from going bad, i.e., people can be helped with their problems.

Observers: Researchers who observed briefings reported that only 62% address insider threat and volunteer spies. For those who do, they discuss quite frequently the causes of volunteer espionage and the presumed motives of known offenders. Less frequently do they document the fact that that most espionage is committed by volunteers.

Personnel Security Indicators and Vulnerabilities

Providers: Seventy-two percent of providers reported that they address this topic and 82% of these individuals feel that they do a good job. They generally list the classic kinds of reportable behaviors, or situations that would lead a person to suspect a coworker was about to commit espionage or was already involved. Among the characteristics mentioned by different providers were changes in attitude or demeanor, financial problems, troubles at home or on the job, low self-esteem, suspicious or unusual behavior, disgruntlement with work, espousing the ideology of the other side, drug or alcohol abuse, excessive gambling, psychological/emotional problems, and sexual misconduct. Additional characteristics include unexplained affluence, staying late at work, excessive use of copying machines, asking for access to information for which a person has no need to know, vulnerabilities to ethnic targeting because of cultural background, travels/contacts, romance, gullibility, etc. Only one person mentioned blackmail. Mention is made fairly frequently of the need to intervene if possible with troubled people, to get them into a support system, to help them personally, and thus to prevent espionage.

Providers teach their audiences how to identify suspicious behavior, and that they must then report it. Examples of suspicious behavior are requests for classified information outside the scope of normal duties or the removal of classified material from the workplace. Case material makes these situations come alive, and providers use these stories as much as possible to illustrate their points.

Observers: Researchers report that 75% of the briefings they observed addressed personnel security indicators and vulnerabilities. Most of the providers covered examples of reportable behavior, informed their audiences of their obligation to report suspicious activities by outsiders and insiders alike, and instructed audience members how to report.

Use of Espionage Case Studies

Providers: Seventy-eight percent of the providers use case studies. And almost 90% of these believe they do a good job with them. Case studies are used for illustration. Sometimes older cases are used if the case illustrates current agency policies; and there are often legal constraints on discussing open cases. But several providers want to see cases from the 90s, to illustrate the fact that espionage still continues and spies continue to be caught. Cases help to show a spy's motivations and whatever personal crisis triggered the espionage. Through cases providers can show the progression of the espionage career. Providers often end the case with discussions of the prison sentence and the damage caused to the country. Cases help to bring home the lesson of the severe consequences to individuals committing espionage.

Observers: Observers reported that case studies were used most frequently when discussing the source of the threat and personnel security indicators. They were used less often to illustrate threat and security countermeasures, the types of information being targeted and consequences of espionage for the nation. When addressing vulnerabilities during foreign travel, modus operandi of foreign intelligence services, and consequences of espionage for the offender, family and friends, case materials were used relatively infrequently.

Impediments to Effective Communication of Threat Information

We asked providers to identify factors that inhibit the successful dissemination of FITA information in their agencies. We also asked them to suggest things that could be done to improve the communication of threat information. They shared their views on a number of subjects, here organized into the major categories into which their remarks fell.

Post-Cold War Climate

One of the major problems in getting the message across is a general perception, among all levels of audiences including senior management, that with the end of the Cold War there is no longer a foreign intelligence threat problem. In addition, it is often difficult to get audiences to grasp the concept of the new, nontraditional threat--our friends and allies and a plethora of newly emerging countries who are interested in acquiring U.S. high-technology. Because they do not believe in the danger, audiences are often "unwilling customers," with a high degree of skepticism and apathy and, thus, inattentiveness.

In addition, in the present political climate, openness and information-sharing are encouraged for the purpose of developing new international business partners and increasing the U.S. share of international trade. Also, scientists desire to share information with their foreign counterparts. This trend toward openness leads to conflicting messages. For example, classified equipment, which traditionally people have been trained to protect, is now often being used in joint ventures with foreign countries and in that context is no longer classified. These new issues are troubling for providers and present them with a challenge as they develop their FITA messages.

Emphasis on Threat Awareness

Related to the above point--unwillingness to believe that there is a threat in the post-Cold War era--our respondents feel there is a lack of management emphasis on awareness activities and little clear policy direction within agencies. Counterintelligence and security are often seen as unimportant, few resources are earmarked for them, and they are poorly coordinated. Sometimes these programs are simply check-the-box items. More management emphasis and personal involvement should lead to policy that will provide adequate budgets for staff and materials, better space for instruction, and more

time to cover the subject. Another problem mentioned by a few providers is that they are facing competition from other educational programs in their agencies, such as EEO and Violence in the Workplace presentations.

Top management, our respondents feel, must take the threat seriously, as seriously as they would a budget, and recognize the importance of security. They must continue to provide adequate resources on a consistent basis, and they must be involved in security, including not absenting themselves personally from briefings. Some providers believe that the government should create standard counterintelligence awareness policy for all agencies to allow for more uniformity across agencies.

Access to Threat Information

Some providers lack interesting, relevant and timely material for use in their briefings. They want access to good information such as case studies, and they want to develop and use multiple sources for information, such as INTELINK, open sources, and POCs in other organizations from whom to request information. They lack specific examples of foreign intelligence services' collection methods, especially how FISs gather information from unclassified sources; they want more information on what is being targeted, how and why; and they lack information on the nontraditional threat.

Other inhibitors include the classification system itself because it does not allow providers to give current examples. Also it prevents providers from acquiring current information regarding the nontraditional threat. They need this fresh information to help capture audiences' interest.

Providers want to see ways of improving collection and dissemination of threat information on a routine basis, with faster dissemination to the field of headquarters-produced threat information. E-mail can be used, or agencies could begin a security provider interest page on the Internet; yet not all providers have Internet access in their offices. They want more and quicker access to secure databases. They need more and better videos and computer-generated products.

Many mentioned they would like to see the creation of a centralized information source, a kind of threat homepage that would include threat information, training sources and materials, general information sources, available briefings and who to contact for briefings, what's new in security, status of regulation changes, etc.

They would like to see more information exchange, more cross-communication and sharing of information among government agencies with a need to know. They want to open more fully the connections across agency borders and disseminate information as widely as possible. Some thought that perhaps the openness could begin with the convening of a formal conference of the counterintelligence components of the various government agencies to share information with each other. (Note: Such conferences do occur regularly, but information about them does not always flow down to the ranks.)

Respondents would like to see new creative ways of disseminating information that are less costly, where the material comes more frequently (at least once a month), and where the information is dynamic and responsive to changes in the threat. They would like to obtain such information without their having to ask for it each time.

Providers' Qualities and Skills

As reported earlier, some providers report they are not properly trained and often do not know where to find source material. Security is often a collateral duty and one in which the new provider has no experience. They indicate that agencies need to provide more formal training, not only in traditional foreign intelligence services' collection methods, but in the modus operandi of nontraditional threat entities.

Instructional Resources

Some respondents say they lack state-of-the-art technology to make their presentations dynamic and to create really good handouts, posters, and brochures. Audiovisual equipment for some is poor and they also lack a source of good videos.

Requests were made for generic briefing slides so the field can augment them. In addition to agency-specific briefings, some respondents would like one common briefing that would work across agencies, and they recommend the development of a variety of scripts or suggested formats for briefings. They would also like a supply of governmentwide posters that are changed more than once a year. Providers from agencies other than DoD recommend more professionally developed videos be produced that use current dynamic examples, that relate to all levels of personnel, and do not always focus just on DoD agencies.

Effectiveness of the Fita Message

We assessed the effectiveness of the FITA message by gathering information from three major sources: the audience receiving briefings, independent observations of briefings, and evaluation of a sample of materials and products used in FITA activities.

We took two approaches to obtaining audience evaluation: we conducted a series of audience surveys and facilitated a small number of focus groups.

Audience Evaluations

Audience Survey

A total of 1,401 audience surveys were collected from briefings conducted by 18 separate agencies. Emphasis was placed on obtaining surveys from all agencies with sizable programs, including all DoD and intelligence agencies. For some agencies, more than one audience survey was conducted. In some instances personnel from more than one agency were in attendance at the briefing.

Table 4 indicates the types of briefings and the number of audience surveys obtained. By far the most frequent type of briefing from which we obtained surveys was the threat awareness briefing. There were two multiple-purpose conferences (145 audience surveys) where more than one type of briefing was presented.

TABLE 4
Surveys by Type of Briefing

Type of Briefing	Number of Audience Members Responding	%
Threat awareness	796	57
Security refresher	253	18
Initial security	156	11
Multiple-purpose conference	145	10
Foreign travel	46	4
Total	1,396*	100

*Five did not designate what type of briefing

Of the 1,275 audience members who responded to a question asking them to rate the briefing overall, both in terms of content and effectiveness of the presentation, 75% rated the briefing as excellent or above average. Only a small number (9%) felt that the briefing was below average or poor.

Table 5 summarizes the percentage of respondents who agreed or disagreed with statements concerning the briefing objectives and presentation quality of the briefings.

TABLE 5
Rating of Briefings by Audiences*

Statement	Agree/ Strongly Agree %	Strongly Disagree/ Disagree %
Briefing Objectives		
Made a convincing case that foreign intelligence activity is a serious concern	94	2
Made a convincing case to report incidents of concern	91	3
Covered specific examples of suspicious activity	89	3
Clearly spelled out indicators of possible foreign intelligence interest or activity	89	3
Explicitly advised me of my obligation to report suspicious behavior and to whom	89	3
Specifically described situations where I might be a target	80	5
Will help deter individuals from committing espionage or other deliberate security breaches	69	9
Clearly defined how my own behavior, especially while in foreign countries, may unintentionally attract foreign intelligence interest	67	12
Presentation Quality		
Was credible	94	1
Was well-prepared	92	2
Had clear objectives	91	1
Was presented in an interesting fashion	84	4
Was relevant to me in terms of my job	84	3
Used aids (e.g., videos, handouts) that were good	80	6

* Most members of the audience answered all questions. Number of responses to these questions ranged between 1,286 to 1,397. Row percentages do not sum to 100% because respondents who neither agreed nor disagreed were excluded.

The data in the table present a very strong endorsement of the providers and the credibility of the information provided. There were only two items for which there was less than an 80% rate of endorsement. One dealt with deterring people from committing espionage and the other with foreign travel. It is probable that the latter item was not included in many briefings because the briefing was not meant to deal with foreign travel. If we look at foreign travel briefings separately, we find that 87% of the audience did agree or strongly agree that this topic was well covered.

Focus Groups

Our other approach to examining the audience's perceptions of FITA briefings was to engage a small number of the audience in a discussion immediately after a briefing. Unlike the audience survey, discussed above, where each audience member fills out a questionnaire, a focus group allows audience members to discuss in detail their responses to the briefing. While the focus groups are not statistically representative, this technique produces a richness and depth that cannot be acquired through surveys; it provides excellent counterpoint to the survey. Appendix G-4 lays out our method for conducting focus groups.

Five focus groups were planned for the project, to take place after government briefings in the Washington, DC area. We were intentionally looking for good briefings because we wanted to learn about how people respond in terms of what makes an excellent briefing. So most of the large agencies with highly developed counterintelligence awareness programs in the study were approached and invited to provide a focus group. We selected the five that could be most conveniently arranged.

Three of the five agencies had invited speakers from other counterintelligence agencies to conduct the briefing for them and in fact one provider, a former government counterintelligence expert, was actually contracted from the outside to team-teach a briefing. The types of briefings included one travel;one information security, dealing with threats to technology; two security refreshers; and one threat awareness. Three of the briefings were taught by a single person, one by a twosome, and the last by an in-house three-person counterintelligence awareness team. All five were stand-up lectures, and used different kinds of handouts, viewgraphs and slideshows and, in one case, a video. The audience size ranged from 14 to 171, with a median of 45. Audiences in two briefings were mid- to high-level government employees, and contractors; the other three were mixed--military and civilian--and included all ranks.

The size of the focus groups ranged from 2 to 9. Participants had either volunteered or had been invited by the agency POC. Focus group participants were military or government employees and contractors, and ranged from junior-level to scientists to mid- and high-level managers.

Participants were asked to discuss their reactions to a specific briefing, using as a framework the series of objectives included in Appendix C-1.

As can be seen from Table 6, there was total agreement (by vote) across all five focus groups that the objectives were fully met in the following three areas: Threat Existence, the Provider, and the Overall Briefing. In other words, all five groups felt that the threat was clearly addressed across the board, the providers were effective, and the

overall briefing was excellent. Targeting was felt to be successfully addressed by four of the five groups. Threat Signals, Reporting, and Relevance were judged successfully covered by only three groups. The weakest goal was Deterrence, with only one group agreeing this message was successfully conveyed.

TABLE 6
Focus Group Agreement That Goals Were Met

	Yes	No	Split Vote Within Group
Threat existence Did the briefing convince you that foreign intelligence activities exist, are a serious concern, and are not just an imaginary threat?	5		
Threat signals Did the briefing help you recognize indicators of possible foreign intelligence interest or activity?	3		2
Targeting Did the briefing help you understand the types of situations in which you might be targeted?	4	1	
Reporting Were you convinced to report incidents of security concern? Was your obligation to do so made clear, as well as the procedures for reporting such activities?	3	1	1
Deterrence Do you believe that the briefing will help deter individuals from committing espionage or other deliberate security breaches?	1	2	2
Relevance Was the briefing relevant to your job?	3	1	1
Provider What was your overall evaluation of the provider: Was the provider credible? Well prepared?	5		
Overall briefing What was your reaction to the briefing as a whole? Did the briefing have clear objectives? Was it interesting? Were the aids used in the presentation very good or effective?	5		

In all five focus groups, three of the eight objectives were judged to have been successfully met. For these three we detail some of the reasons given by the focus group participants. And we follow with a discussion of the one objective deemed to be weak, deterrence.

(a) **Threat existence**: Providers used real-life examples and current, relevant case scenarios. They emphasized economic espionage as a new threat and the need to protect information from competitors, even from allied countries. There was discussion about the

fact that unclassified information is being targeted and analyzed and can be as potent a loss as classified information. Further stressed were the vulnerabilities of the Internet from foreign and domestic sources. Finally, there was an emphasis on the threat in the domestic sphere (e.g., problems of tampering with airplane controls, altering medical record databases, etc.)

(b) **The provider:** Providers were well prepared and did not use notes. They quickly established credibility through various means: used good examples that made a potentially boring topic very interesting, and were light-hearted and humorous. They used plain language, not technical jargon, but they did not talk down to a nontechnical audience. In addition, they responded well to the audience, flowing smoothly back and forth from questions to the presentation. They were personally entertaining, appeared enthusiastic, and seemed to enjoy themselves; used good visual aids; kept audiences alert and interested; and used a good mix of verbal and computer-based presentations. In the case of team presentations, the switching between speakers kept the audience's attention because it provided variety.

(c) **Overall briefing:** Focus group members felt that a team-teaching approach was effective, as was the use of multimedia. The briefing was smooth and of a decent length (long enough to make points, not so long that people got bored). The case histories used were more applicable to the audience than "the typical presentation of the Walker case." They liked the use of video because it presented real cases, plus videos were short and to the point. The entire package made the difference--the provider's delivery, the props used, the excellent viewgraphs.

Deterrence was the weak item and stimulated some special discussion among participants. Several of the participants--those who were security professionals--felt that the message was redundant for them, given that they had been previously vetted and indoctrinated. They also felt that a FITA briefing can produce pictures of prison bars and cells and other forms of dire punishment, but it cannot teach people not to betray their country. For most people, they believed, such principles have long been inculcated by a much deeper socialization process. In any case, they felt that nothing much can stop someone who has already decided to commit espionage. Also, such briefings might have the unintended consequence of actually enabling spies to avoid detection, some believed.

But if a deterrence objective is necessary, then the following suggestions were offered: show how many spies are caught and sentenced and imprisoned; show maximum prison sentences; show impact of cases on the nation and on others' lives (e.g., family members, loved ones); show costly and time-consuming impact of a security break (e.g., hours required to evaluate and address the problem); spend more time trying to reinforce reasons for not spying; stress that companies need to emphasize the protection of proprietary information.

In summary, the focus group participants were impressed by these five briefings. While there is always room for improvement, they say, such as more tailoring for

audiences and agency mission, etc., the briefings did convey the threat well and the providers themselves were excellent.

Briefing Observations

The purpose of the briefing observations was to evaluate how well briefings are conducted in the field. Seven researchers observed a total of 61 briefings sponsored by 20 different government agencies. Briefings were either held on government sites or off-site at professional meetings sponsored by government agencies such as DIS or NACIC. Providers came from 25 different government agencies, or were independent contractors. Table 7 indicates the size of the audiences attending the briefings. Most frequent was a group between 26-50, although there were two one-on-one foreign travel briefs, and one audience as large as 250.

TABLE 7
Size of Briefing Audience

Size of Audience	Number of Briefings	%
1-10	8	13
11-25	10	16
26-50	25	41
51-100	6	10
100-250	12	20
Total	61	100

We attempted to include different types of briefings. Table 8 lists the types of briefings we observed. By far the most frequent type was threat awareness. The two multiple-purpose conferences we attended contained nine briefings on different subjects such as intellectual property, OPSEC, INFOSEC, terrorism, etc.

TABLE 8
Type of Briefing

Type of Briefing	Number of Briefings	%
Threat awareness	33	54
Security refresher	4	6
Initial security	6	10
Multiple-purpose conference	9	15
Foreign travel	9	15
Total	61	100

Observers' overall evaluation of the content and effectiveness of the briefings was quite favorable; 72% of the briefings were rated as excellent or above average, and only 7% as below average or poor. In addition to the overall evaluation, each of the briefings was rated on the extent to which the briefing covered the learning objectives, and a detailed evaluation of the presentation was made.

With regard to the objectives, Table 9 indicates that from the observers' perspective most emphasis was placed upon convincing individuals that foreign intelligence activity is a serious concern. While most briefings covered all the objectives, less emphasis was placed on deterring individuals from committing espionage or sensitizing individuals to ways their behavior might attract foreign interest while abroad. Pure foreign travel briefings, however, always addressed this latter point. It should be noted that the absence of coverage of any of the learning objectives in the context of the 61 briefings being observed does not, of course, mean that the objective was not met by other FITA activities in an agency.

TABLE 9
Observers' Assessment of Emphasis Placed on Various Learning Objectives

Learning Objectives	Great or Some Extent %	Not At All %
Convince individuals that foreign intelligence activity is a serious concern	90	10
Describe specific examples of suspicious or improper activity that should be reported	82	18
Persuade individuals to report any incidents of security concern that they might observe	80	20
Help individuals recognize indicators of possible foreign intelligence interest	80	20
Inform individuals of their obligation to report suspicious activity and to whom	77	23
Sensitize individuals to types of situation in which they might be targets	77	23
Deter individuals from committing espionage or other deliberate security breaches	66	34
Sensitize individuals to ways in which their behavior might attract foreign interest	59*	41

*When we look at just foreign travel briefings, this figure rises to 100%.

In addition to learning objectives, we asked observers to consider additional qualities of the live presentations that have more to do with style, organization, speaker's ability, and quality of materials than content. Table 10 presents the observer ratings of the presentations on these 14 separate factors. In keeping with the positive overall rating, providers were seen as credible and interesting, objectives were clearly stated, and briefings were tailored to the audience (who seemed to be paying close attention). Observers indicated that for the most part a convincing case was made for the reality of the threat. Observers agreed with two statements less than the other items: that the message deglamorized espionage and that it reinforced the idea that most people are loyal.

TABLE 10
Observers' Ratings of Presentations

Evaluation Criteria	Agree %	Disagree %
Presenter was a credible source of information	93	2
Objectives were clearly stated or implied in briefing	90	5
Motivational content was tailored to the audience	80	5
Presenter cited authoritative sources	80	7
Briefing made convincing case for reality of current threat	78	5
Audience appeared to pay close attention to speaker	76	5
Briefing was presented in an interesting fashion	72	8
Presenter provided good answers to questions	72	13
Presenter provided sufficient opportunity for questions	71	15
References were made to recent espionage cases	69	18
Materials used in the presentation were very good	59	12
Information was provided about new policy or legislation	56	18
Message deglamorized espionage	36	16
Message reinforced idea that most people are loyal	28	15

Note: Row percentages do not sum to 100% because respondents who neither agreed nor disagreed were excluded.

Materials Evaluation

Another strategy for judging whether an appropriate foreign intelligence threat message is reaching the audience is to examine the physical materials being used to help express that message. Six hundred separate items were accumulated from 27 agencies and from 6 related organizations such as JIGSAG, SAES and NCMS, etc., as our researchers visited the agencies under review or attended conferences. We asked for the agencies' best materials but, in fact, took everything that was offered. Materials were sorted by our research staff into the following categories: videos and slides; briefings; brochures, booklets, and pamphlets; newsletters and bulletins; and course outlines/seminar agendas.

Posters were not evaluated in detail; nor were workaday counterintelligence and security reminders, such as keychains, note pads, etc.

Each item was catalogued, and then the most significant--in terms of immediate relevance to FITA--were examined in detail and evaluated by a three-person multidisciplinary team of experts, with direct career experience in either counterintelligence or security. The majority of products were for general audiences; others were resource materials designed specifically for the counterintelligence professional. Almost all the materials reviewed (91%) were unclassified.

Over 2 days the experts were able to evaluate 60 items from 20 different agencies. These fell into the first three categories: there were 5 videos, 33 sets of briefing materials, and 22 brochures.

Appendix G-6 is the evaluation form used to judge the items. Basically, the evaluators were looking at materials in terms of whether topic areas (those used consistently throughout this study) were emphasized, mentioned, or not covered at all; the quality of content; quality of the presentation; and whether products were appropriate for dissemination widely across government agencies and among government contractors.

We first report overall statistical data, and follow with evaluators' comments and suggestions.

Videos, slides

There were five videos, one of which was classified. The videos were produced by Army MI, DOE, FBI, NCIS and NRO and, in general, covered well the topics they were designed to cover. Evaluators gave the videos an overall excellent grade. The videos were all given the highest mark for quality of content and presentation. Four of the five were recommended to be distributed within government and three to contractors.

Briefing Materials

Of the 33 briefings, 90% were unclassified. They were collected from 14 different agencies, with Army MI being the largest contributor, with eight. The briefings consisted of computer or view-graph slides summarizing the oral briefings.

As our evaluators pointed out, it is difficult to judge a briefing solely from paper copies. Evaluators have no idea of the manner in which the presentations are delivered in the field. However, based on the briefing outlines alone, only 17% of the briefings appeared to emphasize technical and non-HUMINT, 18% consequences of espionage for the nation and consequences of espionage for the offender and 25% the insider threat and volunteer spies.

The quality of content and presentation was mixed: Between 74% and 77% of the briefings were considered average to high in content and presentation quality, respectively. Evaluators recommended that approximately three-quarters of the briefings were worthy to be distributed to government and contractors. They rated the briefings less favorably than the videos, grading 55% of the briefings as above average or average and 27% as below average or poor. This variability in quality between videos and the briefing materials is not surprising. More technical and expensive effort is invested in producing videos than into preparing briefings.

Brochures, booklets, pamphlets

Evaluators examined 22 brochures, collected from 14 agencies. Ninety-five percent of the brochures were unclassified and most focused on single issues or objectives. The topic stressed the most was modus operandi (60%), followed by sources of the threat (47%), types of information being targeted (44%) and security countermeasures (44%). Others topics (insider threat, technical and non-HUMINT threat, foreign travel and personnel security indicators) were in the low 30%s. The least covered topics were consequences for the nation (14%) and consequences for the offender, family and friends (7%). At one extreme, certain products presented important material in a highly professional and entertaining format. The other extreme consisted of materials that, lacking both substance and good form, were considered to be of little threat awareness value. Several items were commendable in terms of format and presentation, but fell short of overall effectiveness due to lack of clarity and of articulated objectives. Again, the true effectiveness of materials could not be accurately established because the impact of the material on the audience would depend in great part on the individual making the presentation in the context of a live briefing.

Yet, compared to the briefings, the quality of content and presentation of all the brochures was rated higher. However, evaluators would only recommend sending about half the brochures to other government agencies or contractors.

Summary of Evaluation of Materials

The evaluators had a sense that on the whole the materials they saw did reflect the shift from the Cold War to an era of nontraditional threat; were current on the targeting of U.S. critical and advanced technologies and nonclassified high-tech information; and informed audiences about what they should report and how. The materials were less successful in emphasizing elicitation and threat to U.S. persons during foreign travel; stressing the most recent technical threats; discussing the insider volunteer spy; and pointing out personal consequences for the spies and the effect upon the nation of the spies' activities.

Certain briefings, videos or brochures effectively communicated the correct message. The following critical elements were always present in such materials: well-stated objectives; a specific statement of the threat (foreign intelligence or insider); clear

instructions on what the audience should look for, and how and when to report suspicious activity, with an explanation of *why* they should report; and an appealing, modern style and format. Other products did not meet key objectives. The message was not always pulled together adequately, was only partially imparted, or was left to the inductive abilities of the audience to figure out. Also, there are significant differences among the various agencies in what employees are told about reporting counterintelligence and suitability indicators to their supervisors.

In summary, the experts were impressed with the large amount of good content. However, this content was often lost in an inadequate and only partially presented message. In addition, differences in the quality and effectiveness of products can be attributable in part to the large number of agencies developing materials, the purpose for which the materials are intended, and the organizational resources allocated to developing products. There are few underlying commonalities among agencies' products.

It was not our aim in this study to develop a full-fledged library or clearinghouse of exemplar materials, but simply to suggest examples of some excellent products for possible emulation by other agencies. We list below a few of the outstanding items encountered among the products reviewed by our evaluators.

Examples of Excellent Materials

Videos, slides

An excellent video observed by our experts, ***Espionage: A Continuing Threat,*** 1995, and produced by NCIS, contains all the elements of a good briefing.

NRO's ***Travel Files*** was found to be particularly valuable because it used vivid stories to illustrate ways in which people can be very vulnerable when traveling abroad.

Briefings

One slide presentation stood out clearly from all the others, as it contained very specific information on the U.S. targets and modus operandi of several specified countries. This briefing by the Army 308th MI, ***Threat to U.S. National Security***, was classified Secret. It contained exactly the kind of target-specific and country-specific information that industry complains it is not getting.

Brochures, booklets, pamphlets

There are many good, effective items in this category being used throughout the community. Following are some of the items reviewed by our experts that were notable:

(a) ***Passport,*** a passport-size booklet prepared by NSA and used or copied by many other agencies, is an excellent general travel advisory related to personal safety,

convenience and comfort during overseas travel. It does not, however, cover the increased foreign intelligence risks while traveling overseas.

(b) ***Guidelines for Protecting U.S. Business Information Overseas***, produced by the Department of State OSAC, provides excellent coverage of the sharply increased vulnerability to foreign intelligence operations to which travelers are subjected when traveling in a foreign intelligence service's home territory.

(c) ***Why We Care: A Guide for Understanding Suitability and CI Indicators***, a brochure published by the CIA, is a comprehensive product urging employees to report CI and suitability indicators to their supervisors.

(d) ***No Good Reasons Not to Report***, a brochure produced by NSA, focuses effectively on a narrow but critically important issue--overcoming employees' natural reluctance to report adverse counterintelligence or security information about a coworker.

(e) The DIS report, ***Recognition of Potential Counterintelligence Issues***, May 1996, is intended only for security officers, not a general audience. It has a comprehensive discussion of modus operandi for collection operations against defense industry and scenarios that indicate hostile targeting or collection. It also has a very complete list of counterintelligence indicators that security officers should be on the lookout for.

(f) CIA's ***Frequently Asked Questions About Security Policies*** is a comprehensive and stringent guideline for reporting unofficial, close and continuing contacts with foreign nationals. It defines "foreign national," "close" contact, "continuing" contact, and cites examples of contacts that should and should not be reported.

(g) The DIS brochure, ***Suspicious Indicators and Security Countermeasures for Foreign Collection Activities Against the U.S. Defense Industry***, May 1997, describes the modus operandi used to collect information on the defense industry. What makes this brochure valuable is how it relates the threat to countermeasures for defense against the threat. For each aspect of modus operandi, this brochure provides indicators for recognizing the threat as well as countermeasures for protection against it.

(h) NSA's brochures, ***Foreign Intelligence Recruitment Approaches,*** January 1996, and ***Espionage and Foreign Travel***, distributed by both NRO and Department of Energy, make a good start toward helping personnel who come into contact with foreign nationals to understand the intelligence spotting, assessment and recruitment process.

(i) Lawrence Livermore National Laboratory provides a briefing paper, ***Counterintelligence Briefing for Laboratory Hosts of Foreign Visitors***, to laboratory personnel who host visitors from sensitive countries. This is a good example of tailoring threat awareness information to a very specific target audience, and getting it to that audience at exactly the time when it is most needed.

Newsletters, bulletins

NACIC's ***Counterintelligence News and Developments*** and DoDSI's ***Security Awareness Bulletin*** are far more productive than other newsletters and bulletins as primary sources of threat awareness information. Availability of these publications on the Internet facilitates broad access to this information.

The View from Industry

The NACIPB tasking to PERSEREC included a request to examine FITA activities among companies contracted to the federal government. We determined that the most appropriate means for collecting this information in a timely manner would be through telephone interviews of representatives of a sample of those companies.

Major industry associations were contacted to obtain names of relevant companies and knowledgeable individuals within companies. Our goal was to include companies involved in both classified and unclassified work. Excellent support in generating this information was provided by NCMS, AIA, and CSSWG. A letter requesting the opportunity to conduct a telephone interview was faxed to 173 companies; 80 responded that they would be willing to participate. Because of time constraints and logistics in scheduling, only 60 of these individuals were actually interviewed. In addition to the interview, individuals were asked whether they would complete a short questionnaire concerning the extent to which threat awareness activities in their facilities address a number of different topics. Responses to the questionnaire were received from 49 companies. These companies did not seem to differ greatly in characteristics from the larger set of 60 who were interviewed.

Most respondents were corporate directors of security, or security directors of specific programs within the companies. Companies were distributed geographically across the U.S., and manufactured a wide array of military and commercial products. Major government customers were the DoD and the intelligence community, although a broad range of other agencies were also sponsors. Several companies already had contracts with foreign governments; others were presently seeking to expand into the international market.

Respondents were asked to discuss types of audiences, types of briefings and printed material, development of briefings and materials, briefing topics, subject-matter expertise and presentation skills, and give an overall assessment of their program. The latter sections dealt primarily with obstacles associated with disseminating FITA information in the company, and how these problems might be solved.

Types of Audiences

During the telephone interviews, we asked respondents to define their audiences for FITA briefings. Table 11 shows that scientists and professionals are the most common audience, followed by technical and administrative support people.

TABLE 11

Percentage of Respondents Who Report Briefing Various Types of Personnel

Categories of Personnel	Respondents Reported %
Scientific or professional	82
Technical support	37
Administrative support	35
Management	23
Sales/marketing	12
Spouse/family members	3

Types of Briefings and Printed Material

One of the questions we asked industry representatives was the method used to communicate the threat to the audience. Table 12 outlines their responses.

TABLE 12
Method of Disseminating FITA Information

Method	Respondents Reported %
Standup briefings	62
E-mail/computer briefings	30
Videos	28
Newsletters	28
Bulletin boards/posters/displays	28
Handouts/flyers	18
Guest speakers	13

Not surprisingly, as Table 12 shows, traditional standup briefings are the most popular way of disseminating FITA information. Computer e-mail and briefings, videos, newsletters, and bulletin boards, posters and displays are used by approximately one-third to one-quarter of respondents.

Development of Briefings and Materials

Many respondents reported problems in obtaining information to incorporate into their briefings. The most common sources of FITA information are listed below in Table 13.

TABLE 13
Sources of FITA Information for Industry

Source	Respondents Reported %
FBI	58
NACIC	50
DIS	45
State	35
NCMS	27
NSI	27
Newspapers/magazines	27
Commercial threat services	25
Internet	17
ASIS	13
ISAC	13
DOE	12
Customer	12
Security organizations	10
DoDSI	10
Internal	8

The FBI, NACIC, and DIS are at the forefront of providing threat information to industry. Professional security organizations, such as NCMS, ASIS, ISAC, and/or other security organizations, are also cited as sources of information. State Department and NSI were also commonly reported sources. Twenty-seven percent of our respondents reported acquiring information from open sources such as newspapers and magazines; 25% from commercial threat services.

We asked respondents to assess the quality of the information received from each source. With regard to the three major government agencies that are common sources of threat information (FBI, NACIC and DIS), the scorecard is mixed. Some respondents were highly flattering, others neutral, others highly critical. Overall, however, taking into account the realities of shortfalls in staffing and other resources, respondents believe the government agencies are doing their best, often under trying circumstances. They did note that contractors wish to become more of a team with government.

It appears that industry supplements threat information from formal government sources by networking with security professionals from government and industry and participating in industry association activities. They also subscribe to commercial threat analysis services.

Briefing Topics

The questionnaire faxed to industry representatives asked about the extent to which the project's FITA topics were addressed. Respondents were asked to check whether the topics were emphasized, mentioned or not covered at all, and what type of information was presented within each topic. Appendix G-8 contains the topic evaluation form.

Because of the small size of the sample, summarized responses below should not be treated as representative of all industry. Among those contractors who chose to participate in the survey, there was considerable agreement regarding the coverage of briefing topics.

Table 14 shows differences in emphasis among the FITA topics, ranging from about 81% for personnel security indicators to 21% for consequences of espionage for offenders and their families and friends. However, if we combine the percentages in the first two columns, it can be seen that all topics are emphasized or mentioned by three-quarters of the respondents for two topics and by approximately 90% or more for the rest. The last three topics in Table 14--technical and non-HUMINT threat, threat and security countermeasures, and consequences of espionage--were clearly not covered as well as the others.

TABLE 14
Topics in Industry FITA Briefings

Topic	Emphasized %	Mentioned %	Not Covered %
Personnel security indicators	81	19	0
Vulnerabilities during foreign travel	74	24	2
Sources of the threat	67	33	0
Modus operandi of foreign agents	57	39	4
Insider threat and volunteer spies	49	47	4
Types of information being targeted	40	54	6
Technical and non-HUMINT threat	29	59	12
Threat and security countermeasures	23	51	26
Consequences of espionage for nation/offender, family and friends	21	53	26

For some topics, respondents frequently reported addressing a number of current and relevant issues. For example, when discussing personnel security indicators, most inform target audiences of their obligation to report (and to whom) any suspicious or improper activity by outsiders and insiders. They also review specific examples of suspicious or improper activity that should be reported. With respect to foreign travel, most respondents provide general guidelines for the U.S. traveler at a foreign location to counter the espionage threat as well as examples of covert search and theft or compromise of classified or proprietary materials while en route or at hotels. Also covered are examples of the targeting of U.S. citizens, even in allied countries, and technical surveillance measures directed at U.S. citizens abroad. In discussing sources of the threat, respondents indicated that they emphasize examples of countries involved in intelligence operations against U.S. interests, including case examples of allied countries involved in intelligence operations. They also provide audiences with examples of threats from nonstate entities such as foreign organized crime, terrorist groups, and foreign companies.

For other topics, however, some important current issues receive less emphasis. For example, when addressing consequences of espionage for the nation, little concrete sanitized information from classified or non-open official sources about damage incurred by loss of information is presented. When discussing consequences of espionage for the offender, family and friends, case examples are used infrequently. Such examples would be useful in portraying the level of despair and suffering by persons directly or indirectly involved with espionage. When discussing threat and security countermeasures, specific lessons learned from security failures leading to adoption of security countermeasures are not frequently provided. And finally, when discussing the technical and non-HUMINT

threat, little attention is given to other non-HUMINT intelligence collection methods, such as IMINT and SIGINT, or to the technical threat and reasonable countermeasures to minimize electronic eavesdropping.

The coverage of pertinent issues is mixed for some topics. For example, when they discuss modus operandi, respondents place little emphasis on defining ethnic targeting and providing specific case study examples. A better job is done describing techniques for eliciting information and on cautioning against work-related discussions with foreign representatives. When addressing types of information being targeted, high-priority targets (e.g., based on the NSTL) and the current interest in dual-use and economically significant technology receive less emphasis than discussions of specific technologies which have been targeted in the past. Finally, when addressing the insider threat, motives and causes for volunteer espionage are often covered, but the fact that most espionage is committed by insiders is less frequently addressed.

Subject-matter Expertise and Presentation Skills

We asked industry security professionals if they felt they had the subject-matter expertise and presentation skills necessary to perform their jobs. While not all of them conduct briefings themselves nowadays (they are senior people who often have staff who do the briefing), all reported in the affirmative. Most had more than 10 years of experience in security and some had even been trained and formerly served as counterintelligence agents in government. Generally, though, our respondents have a strong foundation in physical and personnel security, but less expertise with foreign intelligence services specifically. Some tend to just pass along to their employees whatever relevant information they receive rather than develop a formalized FITA program.

Overall Assessment

Much of the interview time was spent discussing the obstacles industry faces in the effective dissemination of FITA information and respondents' recommendations for overcoming these obstacles. Nearly all returned to the issue of obtaining relevant and current threat information.

While generic information is adequate, most respondents would prefer relevant--regional-, technology-, industry-, and even company-specific, and often classified--information. Some believe that classified should be distributed widely, others that it should be shared with a company only when that company has a need to know, i.e., when it is being targeted. This information, if not classified, should at least be timely. It must also be credible, not only to satisfy sophisticated audiences, but also to raise the awareness of senior management so that they will put appropriate safeguards in place. Respondents stated they would like the material to be packaged in a digestible and attractive fashion.

Government, according to several respondents, is still holding back threat information. Clearly, not all information can be shared, they agree. Yet industry would just like more. Many suggested establishing a central distribution center to communicate specific threat information in a timely fashion. Other suggestions included providing a list of resources, regular threat assessments, more briefings by government counterintelligence experts, partnerships with the government intelligence community, more videos, and newsletters containing classified threat information to those without access to the Internet.

A second major concern among industry, as companies look towards international markets, is the problem of protecting not just classified but proprietary information. An increasing amount of business is being conducted with representatives of foreign countries. Industry seeks up-to-date, country-specific threat information so that their employees, when exposed to potential vulnerabilities when working with business partners from other countries, can be informed.

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

FITA programs in the Executive Branch and among government contractors are generally effective. For the most part, briefings and instructional materials are adequate or better. Some variability is not surprising given the diversity of agencies' missions, and the number of individuals with varying backgrounds and inevitably different degrees of talent who have responsibility for FITA training. Overall, we found the requisite topics were covered quite well in FITA presentations, the briefing objectives achieved, the presentations well received by audiences, and some high-quality instructional materials available.

More specifically, we conclude that:

1. **Presentation content is up-to-date and reflects the post-Cold War climate. But greater emphasis is needed on the issues of insider threat and personnel security indicators.** In recent history, most espionage has been conducted by insiders who volunteer their services to a foreign intelligence service. The information revolution, post-Cold War openness, global economic competition, new and nontraditional intelligence adversaries, and certain other social and economic trends all combine to create an even more fertile ground for volunteer espionage. Audiences should learn this fact and must be taught to spot the characteristics of a person that indicate he or she might be a security risk.

2. **A significant obstacle to fully effective FITA programs is a lack of access to current information on a number of topics.** Providers in both government and industry report a need for current information concerning not just traditional threats, but the nontraditional threat, economic espionage, computer hacking, etc. They want more detail about what technologies are being targeted, and how and by whom. And they seek a centrally monitored place to obtain such information: a database or a homepage where they can find relevant and current threat information, classified or otherwise.

3. **Objectives used as benchmarks in this study are largely being achieved with one notable exception--discouraging and deterring individuals from committing espionage.** We believe that more emphasis on this objective is required. The message should deglamorize espionage and focus on the high probability of detection and the adverse personal impact of betrayal on the offender, family and friends.

4. **Presentations, for the most part, are well received by most audiences.** Despite negative reactions to FITA from some "unwilling customers" who believe that there are no longer foreign intelligence threats, most people endorse the providers and the credibility of the information provided. While most providers say they are adequately prepared for their responsibilities, more than half indicated a need for more training in

presentation techniques. Also some are eager to improve their presentations with modern instructional aids and materials; to get away from the "crooked vu-graph" technology.

5. **On the whole, instructional materials provide good content**. However, the content is sometimes lost in an inadequate and only partially presented message. Guidance is needed to help providers develop their own materials. Improved means for disseminating high-quality instructional materials also are needed.

6. **More detailed and current case study information is required**. It is not necessary to reiterate a spy's entire life history in a briefing; rather, specific information from cases, old and new, can be extracted to illustrate certain points that a provider would want to make, such as a spy's motivations, reporting suspicious behavior, or explaining the sad consequences of espionage, for the nation or offender. People relate to case histories more easily than to general statements. Old cases can certainly help to teach these lessons, still relevant today. Newer cases, of course, may be fascinating to audiences, but will have little instructional value unless they are related to specific learning objectives.

7. **In some cases in an organization coordination between counterintelligence and security functions is good and in others, where these functions are separated, less effective**. Given that betrayal by insiders is a principal threat, the distinction between threat awareness and security awareness to a large extent disappears; this makes essential the close coordination between counterintelligence and security professionals for exchange of information and planning of FITA activities.

8. **Management emphasis on, and support for, FITA is uneven**. In some agencies, managers are personally involved in FITA activities and provide the resources required for developing good materials and allocating the time to cover material adequately. NSA's re-awareness program is a possible model for some agencies to follow. It integrates re-awareness training into the security clearance (periodic reinvestigation) process and demonstrates management support for the program. Managers in some agencies, however, sometimes take the threat less seriously and, thus, tend not to provide adequate support for the program. Some even are said to treat FITA as a check-the-box requirement. Such an attitude means that fewer resources are allocated to FITA programs. This cavalier approach also can trickle down the system to the rank and file who in turn may learn not to take FITA and reporting responsibilities seriously.

Recommendations

1. Improve the quality and accessibility of threat information

Providers consistently indicated their need for interesting, relevant and timely threat awareness information that can be readily adapted for use in their briefings and instructional materials. They also desire speedy and convenient access to current threat data. Availability of these data through automated networks would facilitate widespread access for providers and afford a more rapid and consistent portrayal of the foreign intelligence threat throughout government and industry.

(a) *To improve the quality of threat information for use by FITA providers, the counterintelligence community needs to devote more attention to the selection and preparation of information to be shared with providers.*

Getting threat awareness information to providers should be an essential part of the counterintelligence mission; and counterintelligence information-producing agencies should begin to think of FITA providers as part of their overall customer base, clients who constantly need information. To this end, producers should work with their clients to identify the types of information they need and the format they prefer. It may be necessary to *create* materials that are appropriate by sanitizing raw information to design products where just the lessons learned are highlighted and can be shared at the unclassified level.

(b) *To make FITA information more accessible, information must be organized to facilitate retrieval and dissemination.*

Some existing data sources offer good information, but are not formated for easy retrieval. For example, in newsletters information is organized by publication date and not generally indexed by subject. Materials are needed where information is organized and cross-referenced in such a way that facilitates access by FITA providers.

Information, once organized, should then be made accessible to providers. The counterintelligence community has a number of distribution vehicles, such as INTELINK or INTELINK CI, the U.S. Government Extranet for the Security Professional (ESP), and the Defense Counterintelligence Information System (DCIIS), as well as web sites at DIS, DODSI, DOE and NACIC. Through such vehicles, current classified and unclassified threat information can be made available to providers for the development and preparation of briefings.

2. **Principal counterintelligence agencies should provide guidance, additional training, and enhanced supporting products for FITA programs in government and industry.**

Supporting products and services would include the following:

(a) *"How to" guidance for deciding what information to include in presentations and instructional materials.* This guidance would assist providers in making their presentations more relevant to the jobs of audience members, a need expressed by observers and audiences alike. Recommended scripts, generic briefing slides or "suggested formats" should be developed to assist providers in developing their own presentations and materials. Specific guidance concerning what information to present will help providers decide on the topics that are most appropriate for their situation and particular audience.

(b) *A FITA resource catalog* in an unclassified format that describes products and briefing support resources (videos, briefing packages, CBT modules, recurring publications, web sites, and points of contact) specially for FITA, along with specific information about how to obtain all products.

Providers were found to be only moderately prepared to locate resources needed to develop or deliver threat information. Some lack the experience required to know where to find FITA resource materials and services. For others, conducting presentations is a collateral duty and they are unfamiliar with the sources of FITA products and services. Providers need to know how to request products and services pertaining to FITA. They also need more information about sources for training opportunities.

It is recommended that NACIC be the lead agency to prepare and circulate this briefing resource catalog. A start has already been made with NACIC's products catalog (classified), DoDSI's Announcement of Products and Resources for the security educator, and PERSEREC's new version of the Desktop Resource Guide.

(c) *Sample instructional materials.* While instructional materials may provide some good content, the point is often lost in an inadequate or partially presented message. Twenty-five to 50% of providers report that they are not well prepared to design effective presentations and instructional aids. They also say they lack state-of-the-art technology to make their presentations dynamic and to create really good instructional materials. Providers need guidance for preparing their own instructional materials. A catalog of high-quality sample materials in a CD format should be developed for easy adaption. This would increase the quality of instructional materials throughout the counterintelligence, security and intelligence communities. Time and money could be saved because providers would not have to develop materials from scratch.

3. **Develop a series of FITA videos**

More videos and short video clips need to be created, each addressing a critical theme or topic. The FITA resource catalog recommended in 2(b) above would make more accessible the good videos already available. While videos are not as personal as a briefing and cannot be tailored perfectly for a particular audience, they can be a very useful instructional aid in combination with other media such as briefings or printed materials. Videos provide a means to consistently communicate the foreign intelligence threat in a high-quality manner. They are especially useful for smaller organizations that do not develop their own FITA materials. However, they do need to be updated regularly and frequently to maintain their relevance.

4. **Foster greater management support for FITA**

Some providers of FITA information report that lack of management support is undermining their ability to achieve FITA objectives. This problem becomes manifested in inadequate resources, the low priority given to FITA relative to other organizational programs and functions, only perfunctory involvement in FITA activities by managers, and an unwillingness by managers to publicly acknowledge the reality and seriousness of the threat. Lack of support erodes the credibility of the providers of FITA information and may result in some managers sending a message symbolically that the foreign intelligence threat is neither a real nor serious problem--a direct contradiction of the message that providers are attempting to communicate.

Managers need to take steps to increase support in terms of adequate financial resources, sufficient staff and time for FITA activities, and improved oversight. They should become personally involved in FITA activities to demonstrate their importance and help correct the perception by some that there no longer is a foreign intelligence threat now that the Cold War is over. They should assure institutional commitment by having all employees under their cognizance participate in and support FITA activities. Managers need to assure good coordination between counterintelligence and security functions to foster an appropriate exchange of information and planning of FITA activities. Finally, managers should develop measures of effectiveness for FITA activities and evaluate them accordingly.

5. **Provide training for FITA providers**

More training opportunities should be made available to providers. Some providers indicated that they need more training, either in developing the content of presentations or in presentation techniques, or both. The evaluation of the instructional materials revealed that good content is often lost in an inadequate and only partially presented message. There is a need to better prepare FITA providers to develop printed materials, design effective audiovisual aids, bring routine material alive and design effective presentations. Many providers also would like exposure to courses specifically addressing various counterintelligence topics and types of threat information.

Suggested agencies to develop this training are either NACIC or DoDSI. DoDSI's current course, *Strategies for Security Education*, could be reinvented to address FITA training needs.

APPENDIX A

Glossary of Acronyms

Appendix A Glossary of Acronyms

AFOSI	Air Force Office of Special Investigations
AIA	Aerospace Industries Association
ANSIR	Awareness of National Security Issues and Response
Army MI	Army Military Intelligence
ASD	Assistant Secretary of Defense
ASIS	American Society for Industrial Security
CG	Coast Guard
CIA	Central Intelligence Agency
CINC	Commander in Chief
COMSEC	Communications Security
CONUS	Continental U.S.
CSSWG	Contractor SAP/SAR Working Group
C3I	Command, Control, Communications, and Intelligence
C4I	Command, Control, Communications, Computers, and Intelligence
DA	Department of the Army
DCIIS	Defense Counterintelligence Information System
DIA	Defense Intelligence Agency
DICE	Defensive Information to Counter Espionage
DII	Defense Information Infrastructure
DIS	Defense Investigative Service
DISA	Defense Information Systems Agency
DOC	Department of Commerce
DoD	Department of Defense
DoDSI	Department of Defense Security Institute
DOE	Department of Energy
DOJ	Department of Justice
DON	Department of the Navy
DS	Department of State
EEO	Equal Employment Opportunity
E.O.	Executive Order
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FIS	Foreign intelligence service
FITA	Foreign intelligence threat awareness
HUMINT	Human Intelligence
IMINT	Imagery Intelligence
ISAC	Industrial Security Awareness Council
ISP	Intranet for the Security Professional
JIGSAG	Joint Industry-Government Security Awareness Group
JS	Joint Staff
MC	Marine Corps
MOU	Memorandum of Understanding

NASA	National Aeronautics and Space Administration
NCMS	National Classification Management Society
NACIC	National Counterintelligence Center
NACIPB	National Counterintelligence Policy Board
NACOB	National Counterintelligence Operations Board
NCIS	Naval Criminal Investigative Service
NIMA	National Imagery and Mapping Agency
NISPOM	National Industrial Security Program Operating Manual
NRC	Nuclear Regulatory Commission
NRO	National Reconnaissance Office
NSA	National Security Agency
NSC	National Security Council
NSI	National Security Institute
OAC	Overseas Advisory Council
OPSEC	Operations Security
ORCON	Originator Controlled
OSAC	Overseas Security Advisory Council
OSD	Office of the Secretary of Defense
OSIA	On-site Inspection Agency
PDD	Presidential Decision Directive
PERSEREC	Defense Personnel Security Research Center
POC	Point of Contact
SAEDA	Subversion and Espionage Directed Against the U.S. Army
SAES	Security Awareness and Education Subcommittee
SAP	Special Access Program
SAR	Special Access Required
SCI	Sensitive Compartmented Information
SIGINT	Signals Intelligence
SPB	Security Policy Board
DOT	Department of Treasury

APPENDIX B

Project Team

Appendix B Project Team

PERSEREC

James A. Riedel, Ph.D., Project Director
Suzanne Wood, Researcher

BDM INTERNATIONAL

Martin F. Wiskoff, Ph.D., Senior Researcher
Susan E. Hodgins, Researcher

Subcontractors:

Richards J. Heuer, Jr., retired CIA Intelligence Officer
Joanne C. Marshall-Mies, Swan Research Inc., Researcher
Anthony R. Palumbo, retired FBI Special Agent
W. A. Sands, Chesapeake Research Applications, Researcher
C. R. (Chuck) Torpy, retired AFOSI Senior Executive

APPENDIX C

Foreign Intelligence Threat Awareness

Appendix C-1 Foreign Intelligence Threat Awareness Learning Objectives

The foreign intelligence threat awareness (FITA) program addresses efforts by foreign intelligence services, foreign commercial enterprises, foreign terrorists, or foreign computer intruders to acquire U.S. classified, sensitive, or proprietary information or materiel, and the unauthorized disclosure of such information or materiel to foreign sources.

We suggest that the specific objectives of the FITA program are, or should be, as noted below. We used these objectives as the standard against which to judge the effectiveness of the FITA program including, specifically, the effectiveness of FITA briefings. We worked with counterintelligence experts in compiling this list, which was later vetted through various of our points of contact at the agencies under review in this study.

1. To convince personnel that foreign efforts to acquire U.S. classified, sensitive, and proprietary information or materiel are a serious concern that affects us all, and not an imaginary or outdated threat.

2. To sensitize personnel to ways in which their own behavior, especially in foreign countries, may unintentionally attract foreign intelligence interest.

3. To enhance employees' ability to recognize indicators of possible foreign intelligence interest or activity.

4. To sensitize personnel to types of situations in which they may be vulnerable to foreign intelligence activities, and inform them how to behave to protect security and their own safety.

5. To inform personnel of their obligation to report indications of suspicious or improper activity to appropriate authorities; to identify what should be reported and to whom, and to motivate personnel to make such reports.

6. To deter betrayal or other deliberate security breaches by our own personnel and to deglamorize spying for a foreign government or group by pointing out that espionage it is committed by troubled individuals, it usually makes their problems worse, they are usually caught, and punishment is severe.

Appendix C-2 Foreign Intelligence Threat Awareness Topic Areas

In conjunction with our project advisors, we devised a list of topics appropriate to be covered in FITA briefings and other activities. The list was vetted through several of our points of contact at the various agencies under review and was subsequently used frequently in this study.

Sources of the Threat

Examples of countries involved in intelligence operations against U.S. interests.

Case examples of "friendly" countries involved in intelligence operations against U.S. interests.

Examples of threats to U.S. information from non-state entities such as foreign organized crime groups, terrorist organizations, and foreign companies.

Modus Operandi of Foreign Intelligence Agents and Services, and Collectors that Target U.S. Persons

Description of techniques for eliciting information.

Definition and case study examples of ethnic targeting.

Caution to limit discussions of one's work with foreign representatives.

Types of Information Being Targeted

Review of high-priority targets (e.g., based on the National Security Threat List [NSTL]).

Review of specific technologies that have been targeted and supporting evidence.

Outline the current interest in dual-use and economically significant technology.

Insider Threat and Volunteer Spies

Documentation that most espionage is committed by volunteers.

Review of causes of volunteer espionage (e.g., financial problems, alcohol abuse).

Identification of presumed motivations of known offenders (e.g., greed or revenge).

Preceding Page Blank

Personal Security Indicators

Inform target audience of its obligation to report any suspicious or improper activity by *outsiders*, and to whom to report.

Inform target audience of its obligation to report any suspicious or improper activity by *insiders*, and to whom to report.

Review of specific examples of suspicious or improper activity that should be reported.

Technical and non-HUMINT Threat

Discuss the intelligence targeting of encrypted voice, fax and data communications.

Review current threat to restricted information systems and computer networks posed by hackers.

Review and define other non-HUMINT intelligence collection methods (IMINT, SIGINT, etc.)

Consequences of Espionage for Nation; and for Offender, Family and Friends

Specifics about damage or potential damage to national security from recent espionage cases, quoting media or other open sources.

Concrete information from classified or non-open, official sources about damage incurred by loss of information, if sanitized.

Types of damage possible from espionage: loss of life, intelligence systems, diplomatic negotiating strength, military advantage, economic opportunities.

Use of case examples to portray the level of despair and suffering by persons directly or indirectly involved with espionage.

Cite case studies which illustrate severity of imprisonment in serious cases.

Vulnerabilities During Foreign Travel

Discussion of technical surveillance measures directed at U.S. citizens abroad.

Examples of targeting of U.S. citizens, even in "friendly" countries.

Examples of covert search and theft or compromise of classified or proprietary materials while en route or at hotels.

General guidelines for the U.S. traveler at a foreign location to counter espionage threat.

Threat and Security Countermeasures

Explain the rationale for security countermeasures in terms of specific threat information.

Show how lessons learned from specific cases have led to the adoption of security countermeasures.

Appendix C-3 Foreign Intelligence Threat and Security Awareness Topics

The following describes substantive topic areas which provide content consistent with the objective of delivering relevant, current, and accurate threat information to employee populations. Several of these content areas focus on the *nontraditional threat.* This central idea can form the theme of an up-to-date threat briefing in which the presenter compares how we perceived the foreign threat in the 1960s and 1970s with how we see it today, in the post-Cold War era, in terms of sources, targeted information, and modus operandi. Espionage cases which serve as relevant examples follow in brackets after several paragraphs.

Sources of the Threat

The adversarial threat is more complex now than that frequently described in threat advisories during the Cold War era. Gone is the bi-polar world of free versus communist or Soviet-bloc countries. Although the Russians and their intelligence services remain a significant threat, we must recognize that there are now a multitude of nations, commercial organizations, and non-national entities that pose a threat to our critical or classified information. In situations that involve economic competition, even national level organizations of what we consider to be friendly nations can actively attempt to acquire U.S. commercial information and technology by illicit methods. The complexity of the adversarial threat must be sketched out with emphasis on the fact that many foreign national and non-national adversarial interests are involved. [Lalas, Brown, Schwartz]

This presents a more sophisticated world-view for members of the employee population to grasp and appreciate. The contemporary intelligence threat has proven to include drug cartels, international crime organizations, terrorist groups, revolutionary organizations as well as freelance former agents of now-defunct Eastern bloc intelligence services. Both classified and unclassified authoritative U.S. government sources have identified several of the most aggressive adversarial countries which target in particular U.S. critical technology, both dual-use and advanced technologies having direct military application.

Quality indicators:

- ✓ Examples of countries involved in intelligence operations against U.S. interests
- ✓ Case example(s) of "friendly" countries involved in intelligence operations against U.S. interests
- ✓ Review of recent Russian activities and intelligence services (GRU, SVRR)
- ✓ Examples of non-state entities targeting U.S. interests
- ✓ Examples of threats to U.S. information from non-state entities such as organized crime

Types of Information Being Targeted

Within the past few years it has become clear that threat awareness briefings must include a discussion of targeted information that goes beyond formally classified U.S. government information. Adversarial interests now target advanced technology and a variety of other unclassified information including private sector proprietary information, OPSEC indicators, economic information, and information on advanced research. [Sombolay, Prasad & Kota, Gaede]

The targeting of U.S. critical technology is in fact the most important shift in the nature of the foreign intelligence threat in recent years. This includes both dual use (microcircuitry, communications technology, and advanced software) and technologies that have direct application to military weapon systems. There are a variety of methods used by adversarial interests to gain this information for both military and economic advantage to the detriment of the U.S. These include illegal export, outright theft of data and source codes by foreign employees, the foreign purchase of U.S. firms, and the hiring of U.S. experts by foreign companies.

Whereas we remain primarily concerned about the protection of U.S. government information, adversarial interests place an increasing priority on advanced technology having military significance and dual use. This information is usually unclassified but protected by export controls. There is also the question of safeguarding the proprietary information of U.S. firms which, if lost to foreign competitors, represents a threat to the viability of our economy.

Briefers should consult the current FBI National Security Threat List (NSTL) for high priority issues and other sources which list advanced technologies which are believed to be high on the collection lists of international competitors who might stop at nothing to obtain this information.

Quality indicators:

- ✓ Review of high-priority targets (e.g. based on NSTL)
- ✓ Recent cases of espionage where critical technologies have been targeted
- ✓ Review of specific technologies which have been targeted and evidence of this
- ✓ Outline of the shift of focus by adversarial interests to militarily significant technology
- ✓ Example of dual-use technology and its military application

The Insider Threat and Volunteer Spies

One of the most important facts about contemporary espionage to convey to employee populations is that most of the cases fall into the category of volunteer spying. The crime is, more often than not, self-initiated. Even by the early 1980s it was clear that volunteer espionage was becoming a more dominant pattern than foreign agent recruitment of vulnerable U.S. citizens. Since then, about 75 percent of the espionage cases have fallen into this category.

Regrettably, there is a tendency in threat awareness information, particularly that provided by counterintelligence elements, to focus on external forces (foreign intelligence services and their agents) as the principal instigators of espionage and the cause of the loss of classified information. While intelligence services and *modus operandi* are an important component of the problem, the security educator would be well advised to address foreign agent involvement in the context of the human vulnerabilities and (often) initial actions of those having access. [Lessenthien, Cavanagh, Pitts]

Recruitment is certainly not out of the picture, particularly in the international marketplace where the lure of large "consultancy fees" may lead an engineer or executive to illicitly share proprietary information. But in those known instances involving the loss of classified government information, recruitment for espionage has sometimes meant the recruitment of U.S. citizens by other U.S. citizens having access.

These disconcerting facts have important implications for threat awareness and security education. We need to present these issues to our audiences: Why would supposedly trusted employees and service members voluntarily betray an essential trust? What deterrents should be put in place to minimize the possibility of this happening? And how can the problems of apparently distressed or confused employees be addressed before they go to the extreme of doing something self-destructive?

In discussing these issues with employee populations, the security educator should attempt to establish an appropriate balance between human vulnerabilities and the activities of external predators (which in many cases have simply responded to overtures by a U.S. citizen who has decided to betray a trust).

Quality indicators:

- ✓ Appropriate balance in the focus on employee vulnerability vs. external agents and foreign intelligence services
- ✓ Review of frequency and causes of volunteer espionage
- ✓ Identification of presumed motivations and vulnerabilities of known offenders
- ✓ The use of specific case studies to illustrate the predatory activities of foreign intelligence organizations responding to initial contacts by U.S. citizens.

Modus Operandi of Foreign Intelligence Agents, Services and Collectors which Target U.S. Persons

Whereas in years past much was said about steps in the recruitment process, blackmail, and sexual entrapment, recent history indicates that the contemporary emphasis should be increased on elicitation for information and ethnic targeting. As stated above, while there is no indication that foreign adversaries or international economic competitors have abandoned recruitment based primarily on the offer of financial incentive, the recent history of espionage strongly suggests that aggressive recruitment of U.S. citizens for espionage is less evident, and where such recruitment has been successful, it has usually been undertaken by U.S. personnel recruiting other U.S. persons who are susceptible. [Walker and Conrad spy rings]

Aggressive elicitation for information combined with misrepresentation of identity or interests especially in the international commercial arena is said to be very prevalent at this time. U.S. representatives who have access to any privileged information should be informed of common elicitation strategies and have a clear idea in their own mind about off-limit subject matter for discussion with foreign representatives or even people believed to be domestic competitors or professional colleagues. This level of awareness is particularly important prior to overseas travel or attendance at international conferences.

While ethnic targeting can be controversial, as per the highly publicized DIS memo about Israeli intelligence activities, it is a significant problem and must be addressed. A correct way to handle this might be to present a more sensitive approach in which members of various ethnic communities in the U.S. are mentioned as being targeted by country of origin contacts and agents. But it is important to avoid suggesting that any ethnic or religious community as U.S. citizens might be less loyal than other citizens. [Kim, Pollard, Lalas]

Quality indicators:

- ✓ Description of various types of adversarial agents—moles, sleepers, under-cover, etc.
- ✓ Definition of elicitation for information and use of hypothetical or real examples
- ✓ Definition and case study examples of ethnic targeting
- ✓ Disclaimer of any implied lack of loyalty by any cultural or religions group
- ✓ Reminder of the limits of work-related discussion with foreign representatives and others not authorized access to privileged information

Personnel Security Indicators and Vulnerabilities

Recent studies of why people get involved in espionage lead to the conclusion that we need to be in tune with the people around us, particularly if our coworkers like ourselves have been entrusted with sensitive or classified information. We cannot allow serious signs of emotional or psychological distress to remain unaddressed. The new executive order on personnel security in fact calls our attention to the need to refer troubled personnel to Employment Assistance Programs (EAPs) for reasons including substance abuse and severe financial difficulties. The reporting of coworker behavior which might indicate impairment of judgment should in fact be seen as supportive and in the interest of that person and possibly a moral/ethical responsibility. Vulnerabilities of any type must be addressed before they become a security issue. [Nicholson, Ames]

There is also the issue of coworker and supervisory responsibility for reporting of suspicious and negligent behavior which may indicate that classified information is not being appropriately safeguarded, might be vulnerable to compromise or, at the extreme, espionage may be involved. Examples of suspicious behavior should be described as well as the preferred method of reporting in confidence to a security or counterintelligence professional. [Pollard]

Quality indicators:

- ✓ Review of indicators of possible espionage on the job
- ✓ Vulnerability indicators that demand intervention by concerned coworkers
- ✓ Discussion of employee responsibilities under personnel security programs
- ✓ Description of available EAPs for referral of personnel with serious problems

The Technical and Non-HUMINT Threat

At one time, coverage of other than the HUMINT threat was referred to as "the multi-discipline threat"—an awkward term at best. In our threat awareness programs, we need to look at modus operandi of various types, both HUMINT and SIGINT, or any other method by which potential adversaries are known to be particularly successful. This would include a discussion of (1) the interception of non-encrypted telephonic communications—voice, fax, and data—(2) the penetration of restricted government and corporate computer networks by hackers after sensitive data, and (3) the greatly increased use of technical surveillance devices. These three methods are believed to be very productive for adversarial services and organizations. [West German Hackers]

Quality indicators:

- ✓ Discuss the intelligence targeting of unencrypted voice, fax and data communications
- ✓ Review current threat to restricted information systems and computer networks posed by hackers
- ✓ Review the technical threat and reasonable countermeasures to minimize electronic eavesdropping
- ✓ Review and define other non-HUMINT intelligence collection methods (IMINT, SIGINT, etc.)

Consequences of Espionage:

For the Nation

One of the misconceptions held even by loyal and trustworthy employees is that espionage is some sort of white-collar crime that might mean some paper or accounting losses to government, but not more. In the past we have been unable to portray the extent of damage partly because the extent or nature of the damage itself is highly classified. Falling back on statements from leading law-enforcement officers, such as "The damage from this case is beyond calculation," is not particularly helpful.

What our audiences need to know is something concrete about the magnitude and nature of the loss to our national community. It might be in millions of dollars or numbers of lives, but even in an unclassified mode it is often possible to be more specific. To present this argument that espionage has done real and costly damage to the nation, it may be useful to use case examples with authoritative estimates of damage assessment.

Quality indicators:

- ✓ Specifics about damage or potential damage from recent espionage cases, quoting media or open sources
- ✓ Concrete information from classified or non-open official sources about damage incurred by loss of information
- ✓ Types of damage possible from espionage: loss of life, intelligence systems, technologies, plans, policies, war-fighting capability, sources and methods as well as diplomatic negotiating strength

For the Offender, Family and Friends

At the personal level, the consequences of espionage are comparably destructive. In the past, official guidance has mandated that everyone be informed of the statutory penalties for espionage or for conspiring to divulge national security information. While no more than a brief reference to the U.S. Code, Title 18 might be useful, audience

members must be informed that involvement in espionage activities, especially where serious damage is incurred, has led to life in prison, and during wartime espionage is punishable by death. Using specific case studies and video-interviews, such as *It's Not a Victimless Crime*, our audiences also need to be aware of the intense personal suffering inflicted on family members and friends and that the offenders have essentially ruined their own lives.

A related theme under personal consequence is the very high likelihood of eventual detection of this crime. Several cases have come to light and have been prosecuted in the last couple of years as a result of confidential sources, defections of former intelligence officers, or the availability of foreign intelligence service files following the reunification of Germany. [Schevitz, Nicholson]

Quality indicators:

✓ Using case examples, with video support in live briefings, if feasible, portray the level of despair and suffering by persons directly or indirectly involved with espionage.
✓ Cite case studies which illustrate severity of imprisonment in serious cases.
✓ Stress the facts that offenders have little realistic hope of getting away with the crime in the long run and that serious penalties follow.
✓ Reference to statutory penalties for espionage in U.S. Code, Title 18 and Title 10, Sections 801 to 940, particularly Section 116a of Uniform Code of Military Justice, Espionage.

Special Vulnerabilities During Foreign Travel

While U.S. persons who travel to or through foreign locations should be provided with pre-trip information on special threats and dangers in the areas they plan to visit, general threat awareness should include basic information about the unique threats which U.S. personnel are likely to encounter. In general U.S. travelers are subject to a wide variety of covert monitoring, technical surveillance techniques, and searches of luggage and personal effects. This may take place en route or in hotels. Technical advances in communications and microcircuitry have made it increasingly easy for foreign intelligence services to monitor any traveler through their areas of jurisdiction.

In addition, U.S. representatives may be subject to intensive and aggressive elicitation, and in exceptional cases, provocation and harassment. Travelers to higher-risk areas should be advised not to place themselves in vulnerable situations by engaging in black market activity, illegal currency exchange, substance abuse, illicit sexual activity, or politically sensitive actions or discussions.

Quality indicators:

- ✓ Discussion of technical surveillance measures directed at U.S. citizens abroad
- ✓ Examples of targeting of U.S. official personnel, even in "friendly" countries
- ✓ Examples of covert search and theft or compromise of classified or proprietary materials while en route or at hotels
- ✓ General guidelines for the U.S. traveler at a foreign location to counter the espionage threat

Response to the Threat: The Threat and Security Countermeasures

The nexus between counterintelligence and security countermeasures should be established at various times in a threat awareness program. Concluding threat briefings, videos, or printed advisories with information about how rank and file employees can address the threat provides significance and meaning to otherwise only interesting information. On the security side, adequate coverage of the foreign intelligence threat in a total program of security awareness supplies the justification and motivational element for complying with security rules and regulations that otherwise can seem tedious, pointless, and time-consuming.

Employee empowerment should be an important closing theme of any product or briefing program: "We are not just sitting ducks waiting to be picked off by foreign intelligence operatives; we can stop this loss. This is what we can do…." Thus the focus is shifted from the potential offender and foreign agent to the aware and loyal employee who has clear responsibility for the recognition of vulnerabilities, preventing security violations, timely personal intervention, and reporting. The typical employee, in fact, can be pictured as performing a vitally important role in the counterintelligence process.

Quality indicators:

- ✓ Discussion of the counterintelligence role for all cleared personnel regardless of job
- ✓ Spelling out the link or threat justification for complying with specific rules and policies
- ✓ Focus on specific security countermeasures as justified by examples from case histories
- ✓ Identify specific countermeasures for each of the areas in which foreign intelligence services are said to most effectively obtain U.S. critical and classified information

Other Qualitative Indicators: Effective Presentation Style

In addition to the substantive aspects of the educator's communication to employee populations, the quality and effectiveness of that communication, whether it be by live briefing, newsletter, or video production, can be greatly enhanced by presentation style. The objectives here are to improve attention span; long-term retention of principal ideas, concepts, and arguments; and motivation for supportive performance on the job by recipients of the message.

1. Clear Focus on Employee Performance or Learning Objectives

All too often in the past, threat briefings were padded with "nice to know" details about the structure and staffing of foreign intelligence services, the intrigue of espionage, and spy craft technologies. This glamorization of espionage is counterproductive. In addition, there is an unanswered question for the employee: "What does all of this mean to me?"

In recent years, security educators have become increasingly concerned about security education based on clearly defined performance or training objectives in which objectives are stated before any product or briefing is developed and all that is conveyed to the target population must address a particular objective.

Furthermore there is a good argument for articulating performance objectives right up front to employees so that they are conscious of how this information is supposed to impact on their professional and even private lives.

Quality indicators:

- ✓ Performance objectives identified in the process of briefing development
- ✓ Objectives stated or clearly implied in the content of the product
- ✓ Content makes specific reference to threat information and job-related activities

2. Currency and Timeliness of Information

All are sensitive to dated material that occasionally pops up in videos, canned briefings or written pieces about the threat. References to the Soviet Union or the KGB evoke snickers from some audiences and sometimes ruin the credibility of a presentation. Negative feedback also results from the frequent use of "old" espionage cases. Over the past several years, people have been heard to make comments such as, "If they talk about the Walker case again, I'm going to scream." "Have you got any *new* cases we can tell our folks about?" At the other extreme are security educators who make it a point to plug information about the very latest cases into their refresher or threat awareness briefing. Right now it would be Kim, Pitts or Nicholson. This is a powerful attention grabber for the audience members who conclude correctly that they are getting the latest information.

But currency and timeliness concern not only historical events or the most recent crimes against the nation, but good information about government response to the threat: counterintelligence or security policy changes also enhance the quality and receptiveness of the message.

Quality indicators:

- ✓ Provision for updates and including new case information
- ✓ Mention of latest cases
- ✓ Information about new policy, legislation, or implementation of countermeasures

3. Motivational Content: Direct Appeal to Employee Interests

It is said that employees of different generational groups respond differently to motivational content, e.g., more senior members, who experienced their political socialization during and just after World War II respond to patriotic symbolism whereas baby-boomers may not, etc. Whatever the case, each threat-awareness communication should include motivational content to activate the recipient. If members of the *Me Generation* need an appeal to self-interest or money to get them motivated and interested, that can be accomplished in an awareness presentation. The idea here is that threat briefings should not simply conclude with information about the foreign intelligence threat. Some focus on expectancy of employee response to the threat should not be missing from the presentation: "This is what you can do and this is why you should want to do it."

Quality indicators:

- ✓ Motivational content tailored to meet values of audience: age, occupational status
- ✓ Discussion of damage to national interests resulting from previous espionage
- ✓ Discussion of injury and suffering to offenders, family members and friends from espionage

4. Appropriate Characterization of Target Audience

The question often arising in awareness efforts is: "Who is the target audience and who are we trying to reach with this message?" We had long discussions about this in the planning stages of the Countering Espionage Video Series and came to the conclusion that we are probably not trying primarily to make an impression on the probable offender who for one reason or another will not listen and seems compelled to do something self-destructive regardless of security training. And actually these people are very few in number despite the damage they do. Espionage is in fact a relatively rare crime.

The populations we essentially want to reach and activate are the vast numbers of generally loyal, patriotic, and reliable employees. However, their attitudes sometimes

include indifference to what is going on around them, cynicism about security, and fear or resistance about getting involved in a personnel security situation. These are the attitudes and behaviors we would also like to change or modify.

Consequently, the audience must be addressed as a population of loyal and otherwise responsible individuals. Threats and signs of the "watch-dog—we're out to get'cha" mentality, if expressed by the educators, are sure turn-offs. In general, each message, briefing, or written communication should also be clearly tailored to meet the needs of a particular audience as defined by organizational identity, occupation, educational level, age, or geographical context.

Quality indicators:

- ✓ Content includes reference to group identity or situational factors
- ✓ Signals that briefer or authors view the receiving audience in positive terms
- ✓ Positive reinforcement rather than overly dire warnings directed to the listener

5. The Use of Espionage Case Studies and Other True Stories (Making It Real)

The use of recent espionage case studies or even real examples of how information was compromised (or successfully protected) can illustrate many of the themes mentioned in other topic areas. Each case offers its own lessons to be learned. Case studies also maintain audience attention and interest and provide evidence that espionage is not an other-worldly phenomenon. A risk one runs, however, is to unintentionally glamorize or romanticize espionage as an intriguing thing to be involved in, or to try. Sharing case examples should always include the following: (1) offenders not only risk causing great damage to their nation, but almost always suffer great consequences including lengthy imprisonment, and (2) detection and apprehension is almost inevitable due to the use of confidential sources and advanced counterintelligence methods.

Furthermore the selection of cases to be covered should be made on the basis of currency and commonality with the target audience situation. The discussion of older cases--Bell, Boyce and Lee, or Walker--is by now of questionable value since employees are literally tired of hearing about "the same old cases." On the other hand, a discussion of the very latest espionage events (citing pubic media sources) should earn a favorable learning outcome.

Quality indicators:

- ✓ The use of recent case studies to illustrate one or more points in a presentation
- ✓ The use of a realistic, work-place scenario to show the application of a countermeasure
- ✓ Presentation of case material to de-emphasize supposed romantic or glamorous aspects of espionage
- ✓ The use of cases or event stories most recently in the news and fresh in the minds of the audience

5. Use of Authoritative (and When Possible) Classified Information

The establishment of the credibility of a threat awareness message is essential to ensure members of the employee population will pay attention and display the kinds of performance objectives we are seeking. Credibility, of course, means that the receiver of the message believes that the source of the information is objective and reliable and that the message itself is accurate. Consequently, the crediting of sources such as intelligence organizations, particularly in the presentation of fact that might otherwise sound conjectural, is a very advisable practice.

The question of whether threat briefings should be classified or not often arises. The arguments in favor are these: Much more can be said in detail to support an important argument if the communicator is allowed to include classified information. Because we can mention sources and methods in a classified context, the overall message will be more convincing. And in the area of counterintelligence, much of the important information that employees should know about the threat is either classified or FOUO. In addition, for many people, the mere fact that a piece of information is classified lends credibility and importance to it and, in fact, to the entire presentation or product.

While the latter argument is not by itself a justification for the inclusion of classified material (consistent with the principle of need to know), the need for quality should prevail. That extra effort at developing and delivering a classified presentation on the foreign threat, when it is at all feasible, argues for doing it.

Quality indicators:

- ✓ Mention of authoritative sources where appropriate to lend credibility to facts
- ✓ The identification of respected media sources with the use of open source information
- ✓ When feasible, the development and delivery of information in a classified format
- ✓ The identification of classified facts in the course of a briefing text
- ✓ The use and identification of sensitive information that is not cleared for public release

APPENDIX D

Participants

Appendix D-1 Participating Agencies

Air Force Office of Special Investigations
Army 902d Military Intelligence Group
Central Intelligence Agency
Coast Guard
Commerce
Customs Service
Defense Information Systems Agency
Defense Intelligence Agency
Defense Investigative Service
Department of the Army
Department of Defense Security Institute
Energy
Federal Bureau of Investigation
Federal Emergency Management Agency
Joint Staff
Justice
Marine Corps
National Aeronautics and Space Agency
National Counterintelligence Center
National Imagery and Mapping Agency
National Reconnaissance Office
National Security Agency
National Security Council
Naval Criminal Investigative Service
Nuclear Regulatory Commission
Office of the Secretary of Defense
On-site Inspection Agency
Security Policy Board
Senate
State
Treasury

Appendix D-2 Participating Companies

Aerojet, Sacramento, CA
Alliant Techsystems, Hopkins, MN
AlliedSignal, Columbia, MD
AlliedSignal, Torrance, CA
Atlantic Aerospace Electronics, Greenbelt, MD
BDM International, McLean, VA
Bell Helicopter Textron, Hurst, TX
Boandi Corporation, Phoenix, AZ
Boeing Aerospace Operations, Midwest City, OK
Boeing North American, Seal Beach, CA
Computer Systems Center, Arlington, VA
C.S. Draper Laboratory, Cambridge, MA
Day & Zimmerman, Moorestown, NJ
E.I. Dupont Denemours, Wilmington, DE
Environmental Research Institute of Michigan (ERIM), Ann Arbor, MI
E-Systems, Garland, TX
Frequency Engineering Laboratory, Farmingdale, NJ
GE Aircraft Engines, Cincinnati, OH
GEC-Marconi, Atlanta, GA
GTE Government Systems, Needham Heights, MA
GTE Government Systems, Thousand Oaks, CA
Johns Hopkins University Applied Physics Laboratory, Laurel, MD
Harris Corporation, Palm Bay, FL
Honeywell, Minneapolis, MN
Honeywell/Satellite Systems Operations, Phoenix, AZ
Hughes Aircraft Company, El Segundo, CA
Hughes Defense Communications, Fort Wayne, IN
Litton Guidance and Control Systems, Woodland Hills, CA
Lockheed Martin, Marietta, GA
Lockheed Martin, Salt Lake City, UT
Lockheed Martin Astronautics, Denver, CO
Lockheed Martin Government Electronics Systems, Moorestown, NJ
Lockheed Martin Tactical Aircraft, Fort Worth, TX
Lockheed Martin Vought Systems, Dallas, TX
Lockheed Martin WDL, San Jose, CA
McDonnell Douglas, St. Louis, MO
McDonnell Douglas Helicopter, Mexa, AZ
MIT Lincoln Laboratory, Lexington, MA
MITRE Corporation, Eatontown, NJ
Motorola, Scottsdale, AZ
Northrop Grumman Corporation, Bethpage, NY
Northrop Grumman Corporation, Rolling Meadows, IL

Northrop Grumman Commercial Aircraft Division, Dallas, TX
Olin Ordnance, St. Petersburg, FL
Owens Security Services, Elkhart, IN
QuesTech, San Diego, CA
Raytheon Electronic Systems, Bedford, MA
Raytheon Electronic Systems, Dallas, TX
Raytheon Electronic Systems, Falls Church, VA
Rincon Research, Tuscon, AZ
Rockwell International, Richardson, TX
Sanders, a Lockheed Martin Company, Nashua, NH
Science Applications International Corporation, San Diego, CA
Security Computing Corporation, Roseville, MN
SRI, Menlo Park, CA
System Technology Associates, Colorado Springs, CO
Texas Instruments, Dallas, TX
Thiokol Corporation, Ogden, UT
TRW, Redondo Beach, CA
United Technologies, Hartford, CT

APPENDIX E

Counterintelligence and FITA Authority and Policy

Appendix E Counterintelligence and Threat Awareness Authority and Policy

As with all major matters and missions under the responsibility of the Executive Branch, executive orders set forth policy and parameters for departmental implementation of intelligence and counterintelligence programs in general, to include the foreign intelligence threat awareness programs under review in this study. Broadly worded executive orders are implemented by each department in a manner that complies with the executive order, yet are tailored to fit the particular needs, operating atmosphere and culture of the individual department. Additionally, depending on the size of the department and its perceived vulnerability to foreign intelligence targeting, subordinate agencies and components usually further implement the executive order and their departmental directives to fit particular subordinate requirements. Consequently, the largest departments, such as Defense, will have significant numbers of cascading directives, instructions and regulations that implement the executive order affecting awareness programs down to the lowest major operating level, while the many smaller departments may have no subordinate implementing directives.

The main policies governing foreign intelligence threat awareness activities across the federal government are:

E.O. 12333 U.S. Intelligence Activities, December 4, 1981

This is the primary, if dated, executive order concerning intelligence activities and responsibilities in, and for, the United States. It is a broad policy document that provides for effective conduct of U.S. intelligence activities and was designed to assure that the U.S. receives, by lawful means, the best intelligence information and counterintelligence protection available. The executive order assigns roles and responsibilities to the various members of the intelligence community and other agencies for collecting foreign intelligence information and conducting counterintelligence in the federal government, and for executing the programs in a lawful and nonobtrusive manner concerning U.S. persons.

PDD/NSC-12 Security Awareness and Reporting for Foreign Contacts, August 5, 1993

PDD/NSC-12 is the most relevant directive to our present review of foreign intelligence threat awareness programs. It specifies that each department or agency in the US government must maintain a formal security and/or counterintelligence awareness program designed to:

Ensure a high level of awareness among employees of the potential threat to its classified, sensitive and proprietary information from foreign sources, as well as from inadvertent or deliberate disclosures by cleared personnel

provide for the reporting of certain employee contacts with foreign nationals as required

be tailored to meet the particular functions and vulnerabilities of the agency

ensure no violations of employees' privacy or freedom of association

This program must include periodic briefings, or briefings prior to foreign travel.

E.O. 12356 National Security Information, April 2, 1982

Under this order, the balance between government secrecy and the public's right to access information emphasized secrecy. Executive agencies were instructed to classify any information that reasonably could be expected to cause damage to the national security. This is related to foreign intelligence threat awareness in the sense that it is strongly supportive of strong awareness programs.

E.O. 12958 Classified National Security Information, April 20, 1995

This order prescribes a uniform system for classifying, safeguarding and declassifying national security information, and also establishes a monitoring system to enhance its effectiveness. Various implementing documents direct agencies on how this will be done. It is supportive of sound awareness programs, in that basic understanding of classification systems facilitates good awareness and security.

E.O. 12968 Access to Classified Information, August 4, 1995

This order describes how our system of classified information should be organized in a manner that protects both our citizens and democratic institutions. The document lays out a uniform federal personnel security program for employees who will be considered for access to classified information, specifying that all personnel security programs should include continuing security education and awareness programs.

Memorandum from National Security Council, Early Detection of Espionage and Other Intelligence Activities Through Identification and Referral of Anomalies, August 23, 1996

This memorandum was circulated to the Vice President, State, Treasury, Defense, Justice, Commerce, Transportation, Energy, the US Trade Representative, Office of Management and Budget, Chief of Staff to the President, CIA, and the Joint Chiefs of Staff. It averred that timely recognition and reporting of anomalies[1] to appropriate

[1] An anomaly is defined as foreign power activitiy or knowledge, inconsistent with the expected norm, that suggests foreign knowledge of U.S. national security information, processes or capabilities.

counterintelligence authorities can result in earlier identification of espionage or other foreign intelligence activities. The memorandum instructed recipients to formally structure a process for handling information on anomalies within their organizations that would, among other things, integrate into existing security awareness and counterintelligence presentations information on everyone's responsibilities for early recognition and reporting of anomalies.

Director of Central Intelligence Directive DCID 1/14 Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information, January 22, 1992

This directive addresses screening, access to, and handling of, specialized and unusually sensitive intelligence information on individuals or events, similar to but using much more stringent controls than set forth in E.O. 12968.

Executive orders and other guidance documents are promulgated in the Defense agencies and military services by a series of DoD directives, instructions and regulations. These are the workaday documents governing the Defense Department, tailored for its special purposes, being distilled from the broad executive orders on which they are based. The main policy document for counterintelligence awareness and briefings in the Defense agencies and military services is DoD Directive 5240.6 (immediately below). Several others impacting threat awareness requirements also are mentioned in addition.

DoD Directive 5240.6 Counterintelligence Awareness and Briefing Program, July 16, 1996

This directive, recently updated, requires all DoD employees--military personnel (active and reserve), civilian and DoD contractors--to report information on individuals or events that could pose a threat to U.S. personnel, DoD resources or classified national security information, specifying appropriate authorities to whom to report. The threat, quite different from the 1986 version which focused on communism and specifically designated countries, now includes foreign intelligence, foreign commercial enterprises, terrorists, computer intruders, and actions that result in unauthorized disclosures. This document relaxes a previous requirement for the military services to report numbers of people briefed on threat awareness each year; only the number of incident reports are currently compiled to show trends in foreign efforts against Defense activities.

The directive requires that each DoD component must establish a program to:

keep employees aware of threats to personnel, material and information

keep employees educated about their responsibilities to report these threats

teach employees how to identify reportable situations

Awareness programs are required to involve periodic awareness briefings at least every 3 years, with other methods between briefings to maintain continual awareness of the threat and employees' personal responsibilities.

DoD Directive 5240.2 DoD Counterintelligence, June 6, 1983

This directive is being reissued as it requires updating relative to the policies and responsibilities of DoD components engaged in counterintelligence activities; incorporates DoD counterintelligence into the new national counterintelligence structure; and reinforces the delineation of the roles and responsibilities of the military departments and the combatant commands in counterintelligence. It incorporates and accommodates relevant amendments to Title X, U.S. Code, brought about by the Goldwater-Nichols Act of 1986.

DoD Instruction 5210.84 Security of DoD Personnel at U.S. Missions Abroad, January 22, 1992

This instruction describes the Memorandum of Understanding between the Defense and State Departments at U.S. missions abroad, and the Attorney General memorandum concerning FBI responsibility to conduct investigations of alleged espionage by U.S. personnel assigned to these missions.

DoD Directive DoD-0-2000.12 DoD Combatting Terrorism Program, September 15, 1996

This directive was recently re-written in light of the Khobar Tower incident in Saudi Arabia and is currently being revised again. The aim of this directive is to protect from terrorist acts all DoD personnel and their families, facilities, and other material resources. Commanders and managers are tasked with elevating the awareness of DoD personnel and their families to the general terrorist threat, the specific threat in their immediate areas, and personal protection measures that can reduce personal vulnerability.

The military services have numerous counterintelligence and security-related directives; however, only the ones focusing directly on threat awareness are addressed below.

Army Regulation 381-12, January 15, 1993, describes the SAEDA program (Subversion and Espionage Directed Against the US Army). Emphasis is placed on the importance of conducting counterintelligence education for all Army personnel at least annually; and on reporting SAEDA incidents. Each briefing attendee should know what, when, why, and where to report information. Army personnel should be instructed on the dangers of becoming targets of foreign intelligence activities; criminal penalities for espionage and for not reporting relevant information; methods used by foreign countries to collect information; how to respond to and report SAEDA incidents; and the international and domestic terrorist threat.

Army Regulation 381-10 US Army Intelligence Activities, July 1, 1984, governs the conduct of intelligence activities by the Army intelligence components. It implements DoD Directives 5240.1 and 5240-1R which, in turn, implemented E.O. 12333 and is more concerned with oversight than with awareness specifically.

The Navy and Marine Corps policy is contained in **OPNAVINST 5510.1H Chapter 5, Counterintelligence Matters to be Reported to the Naval Investigative Service, April 29, 1988**. This chapter is dated 1988 and the DON is presently working on a revision. This document describes a program designed to get all military and civilian personnel in the DON, whether they have access to classified information or not, to report incidents regarding sabotage, espionage or deliberate compromise; contacts with citizens of designated countries; suicide of Service members with access to classified information; unauthorized absentees; and certain foreign travel.

The Air Force's policy is found in **AF Instruction 171-101, Vol I, Chapter 3, Counterintelligence and Protective Service Matters, July 22, 1994.** The aim of the Air Force program is to instill in personnel a high level of awareness of the threat to classified, sensitive and proprietary information from foreign sources as well as from inadvertent or deliberate disclosures by any personnel. Initial briefings are given to military and civilians upon their entrance into the Air Force or Air Force civilian employment. Follow-up briefings are to be given to the military upon permanent transfer or at least every 3 years, and to civilians every 3 years. Providers tailor the briefing to the audience and include: the threat posed by foreign intelligence, foreign government-sponsored commercial enterprises, terrorists, and international narcotics trafficking organizations; the threat to specific installations or missions; specific security vulnerabilities of the assigned command; how the threat applies to the installation where serving; and the individual's responsibilities and reporting requirements.

Just like the military services, the other Defense agencies and components develop their own specific policies that implement DoD regulations.

The **Defense Intelligence Agency** (DIA), including the Defense HUMINT Service, is guided by **DIAR 54-2 Counterintelligence: Foreign Intelligence Collections Efforts, Foreign Contacts and Counterintelligence Awareness Program, June 3, 1987**. Another directive, **DIA 54-5 Counterintelligence: DIA Counterintelligence, October 11, 1983**, is currently undergoing revision. DIA is reviewing its threat awareness briefing and expanding it to make it more inclusive and applicable to the workforce. Since 1989, threat awareness through the Defensive Information to Counter Espionage (DICE) briefing dealt exclusively with the espionage threat to DIA and its employees. However, it did not portray adequately the total threat picture. The revised briefing will include, in addition to the espionage threat, material on terrorism, the threat to DIA's information infrastructure, and the perception management threat.

DIA's **DIAM 100-1, Vol. III, dated November 1995,** establishes security standards for the effective administration and operation of a Defense Attache Office. It

defines security-related responsibilities; provides personal, personnel and facility security guidance; identifies security-related resources and investigative support; and establishes reporting procedures. This recently revamped document is issued under the authority delegated to DIA in DoD Directive 5105.21, Defense Intelligence Agency, May 19, 1977.

The **Defense Information Systems Agency** (DISA), in addition to being subject to all the DoD regulations, is guided by **DISA Instruction 240.110.8 Information Security Program, June, 1996**. This instruction lays out the types of security awareness briefings to be offered at DISA. And it includes the Counterintelligence Awareness and Briefing Program, with a discussion of reporting requirements, and the requirements for an annual briefing on hostile intelligence and terrorist threats.

Defense Investigative Service (DIS) **Counterintelligence** is governed in general by the same directives as the larger DoD agencies, i.e., all executive orders and other DoD policy guidance pertaining to counterintelligence. DIS has its own **Regulation 25-5 Counterintelligence and Awareness Briefing Program, April 23, 1987**. This was updated in 1990 and 1991 and a new version is presently in coordination. This regulation basically mirrors the DoD Directive 5240.6. The NISPOM is the DIS "directive" for contractors. The requirements levied on contractors are incorporated into that document.

The **Joint Staff** takes guidance from **MCM 149-92 Chairman, JCS document, Counterintelligence Support, October 26, 1992** which requires that "the Chairman of the Joint Chiefs of Staff...will integrate, where appropriate, counterintelligence support into all of joint planning, programs, systems...when a foreign intelligence threat or domestic threat, as defined by the Department of Defense, exists or potentially exists to joint capabilities or mission accomplishment." JSI (Joint Staff Instruction) 5240.02A, June 30, 1995, *Joint Staff Security Program,* provides guidance on personnel security; procedures are governed by JSM 5240.01A, May 9, 1997, *Joint Staff Personnel Security Procedures Manual*. JSM 5240.01A charges the CJCS with "establishing a defensive security and anti-terrorist protection briefing program, and briefing and debriefing Joint Staff personnel...the (Joint Staff) will coordinate with DIA to arrange for Joint Staff personnel to receive detailed, specific or special briefings on the latest intelligence information. Overarching DoD guidance is provided by DoD Directives 5240.6, 2000.12, and 5240.1R.

On-site Inspection Agency (OSIA) has its own **OSIA 5240.2 Rules and Security Procedures Governing the Conduct of On-site Inspection Agency Personnel, March 5, 1996,** which prescribes rules and security procedures concerning the conduct of all personnel assigned, or attached under contract, to OSIA, on either a permanent or temporary basis, and outlines the rules for briefing travelers. OSIA was

established by NSD296 and is governed by various PDDs and directives regarding the various treaties that it executes. The agency is guided also by other DoD directives, such as DoD Directives 5240.2 and 5240.6. etc.

The **National Reconnaissance Office** (NRO) is guided by E.O. 12333 and PDD/NSC-12, as well as various DCIDs and DoD directives and instructions (e.g., DoD Directives 5240.1R, 5240.2, 5240.6). NRO internal memoranda and directives currently outline reporting requirements for foreign contacts and travel, and set the standards for awareness briefings for affected employees. NRO is presently re-casting two Director's Memoranda (written in 1991 and 1992) into an NRO Directive on Counterintelligence which will address policies, procedures and responsibilities for the NRO counterintelligence program. Requirements for counterintelligence awareness and training for employees and contractors will be specifically addressed.

National Security Agency (NSA) has literally dozens of separate regulations or policy issuances that promulgate the larger policy edicts such as PDD/NSC-12, E.O. 12333, E.O. 12968, DCID 1/14, etc. A few examples are: **Association with Foreign Nationals, Policy Issuance 120-19, October 1995; Security Requirements for Foreign Travel, NSA/CSS Regulation 30-31, October 1994; Individual Security Reporting Requirements, NSA/CSS Regulation 120-15, March 1995; and Handcarrying Classified Material and Controlled Cryptographic Items, NSA/CSS Regulation 123-2, 1995.**

Many non-DoD federal agencies have their own policies that implement executive orders, resulting in foreign intelligence threat awareness policies tailored to fit their own cultures and missions. Some agencies, however, were unable to provide us with copies of policies, generally because they do not have full-fledged counterintelligence briefing programs. Below are examples of how the larger, key agencies have interpreted executive policy.

The **Central Intelligence Agency** (CIA) is guided by a variety of regulations regarding counterintelligence and security. None of the regulations specifically mandates a specific, periodic foreign intelligence threat awareness program. Given the unique nature of the CIA mission, security awareness and foreign intelligence threat awareness have always been considered part of the basic and specialized training programs and daily responsibilities of all CIA employees. After the arrest of Aldrich Ames, the CIA Executive Director issued a classified memorandum establishing the Counterintelligence and Security Program (CISP). The CISP is a mandatory 4-hour briefing for all employees that covers employees' accountability for their own actions, responsibility for reporting suitability and counterintelligence indicators that surface in a colleague's behavior, and an update on the foreign intelligence threat.

The **Coast Guard** (Department of Transportation) has **COMDTINST M5528.1 Security Awareness, Training and Education Program, August 3, 1993**. The goal of the Coast Guard program is to instill security consciousness in all personnel and ensure a

uniform interpretation and application of security standards. The program aims to develop fundamental habits of security to the point that proper discretion is automatically exercised in the performance of duties, and the protection of government assets (classified information, property, and personnel) becomes a natural element of every task.

The **Department of Commerce's** policy documents include **COM DAO 207-1 Commerce Administrative Order Personnel Security and Suitability Program, May 1996,** which authorizes the development of their security manual; **DCID 1/14, Personnel Security Standards and Procedures Governing Eligibility for Access to SCI, January 22, 1992**; and **PDD/NSC-12, Security Awareness and Reporting of Foreign Contacts, August 5, 1993**. COM DAO 207-1, based on E. O. 12958, sets standards for Commerce's security education and training programs.

The **Department of Energy** (DOE) takes policy guidance from **DOE 5670.3 Counterintelligence Program Order, September, 1992.** Chapter 13 of this document establishes policies, procedures and specific responsibilities of the counterintelligence program in the Department of Energy which includes requirements for a comprehensive awareness program.

The **Federal Bureau of Investigations** (FBI), is guided by Department of Justice interpretations of higher-level government-wide policy guidance. Examples are **DOJ 28 CFR PART 17, National Security Information Program, November 7, 1985,** an interpretation of E.O. 12356; and other DOJ directives such as **DOJ Order 2600.2B Security Programs and Responsibilities, July 10, 1989** and **DOJ Order 2640.2C Telecommunications and Automated Information Systems Security, June 25, 1993**. In addition, FBI implements DOJ regulations for itself in such documents as **FBI SAC Memo, Security Awareness Training for All FBI Employees, July 23, 1990**; **and the Manual of Investigative and Operational Guides (MIOG), Part I, Section 260, Security Officer Matters, September 26, 1990.** FBI also works with the espionage statute: Title 18, Sections 641, 793, 783, 798, and 952.

The **National Counterintelligence Center** (NACIC) and the National Counterintelligence Policy Board were established under the auspices of the National Security Council by the issuance of **PDD/NSC-24(S) US Counterintelligence Effectiveness, May 4, 1994.** This directive was designed to restructure U.S. counterintelligence, to "foster increased cooperation, coordination and accountability among all US counterintelligence agencies." It includes responsibility for developing and monitoring the effectiveness of interagency training courses for counterintelligence professionals as well as counterintelligence awareness programs for both the public and private sector. In addition, the National Security Council approved a 7-point program on awareness: this included plans to bring counterintelligence awareness to industry through various training seminars and mass media.

National Aeronautics and Space Administration (NASA) has its own **Security Handbook NGB 1620.3C, February, 1993**. Chapter 22, Security Education and Motivation, lays out the types of security briefings required, including foreign travel briefings. Chapter 41, Threat and Incident Reporting, lists reportable incidents. Field installations translate this overall NASA guidance into specific policies. **Goddard Space Flight Center's GHB 1600.1A Security Manual, November 30, 1990**, is an example. This describes the security awareness education programs, the types of briefings required, and especially the foreign travel briefings and their requirements.

National Imagery Mapping Agency (NIMA) has a regulation, **DMAM 5200.1, September 28, 1987** (closely adapted from the DoD Directive 5200.1, DoD Information Security Program) and an Information Security Program Regulation (which is basically the same as the DoD 5200.1-R.) **DAMH 5200.1, Security Monitor's Handbook, July 1986**, contains information on how to perform the duties of a Security Monitor which include the conduct of a counterintelligence and security awareness briefing program.

The **Office of Security** in the **Senate** was established in 1987 via Senate Resolution 243-100-1, 1987. (This agency is an anomoly in this study since it is part of the Legislative Branch, not the executive.) The Senate has produced a security manual describing the program for all Senate employees which is based on various DoD directives such as DoD 5240.6. The manual discusses the different kinds of briefing requirements for employees and the frequency with which they are to be conducted.

The **Department of State** (DS) derives its overall guidance from the **Omnibus Diplomatic Security and Antiterrorism Act of 1986** and from **12 FAM 260, Counterintelligence, May 5, 1995.** The latter document describes the State Department's counterintelligence program which has as its purpose the deterrence and detection of the threat posed by hostile intelligence services against US diplomatic personnel, facilities and information. Requirements for security and counterintelligence awareness programs and contact reporting are delineated, along with details of travel briefing requirements.

APPENDIX F

Agency Descriptions

Appendix F-1

AGENCY	AIR FORCE OFFICE OF SPECIAL INVESTIGATIONS (AFOSI)
HQ POINT OF CONTACT	Gerry L. Fawley Investigations Operations Officer

BACKGROUND

AFOSI has been the major investigative service for the Air Force since 1948. Its primary responsibilities are criminal investigative and counterintelligence services. The organization seeks to identify, investigate, and neutralize espionage, terrorism, fraud, and other major criminal activities that may threaten Air Force and DoD resources. AFOSI provides professional investigative service to commanders of all Air Force activities. Operations are organized into the following areas: counterintelligence (operations, investigations, collections and production); anti-terrorism; criminal investigations; computer crimes investigations; economic crime investigations; force protection; specialized services and training.

AFOSI derives policy guidance from E.O. 12333 *U.S. Intelligence Activities* (Dec 4, 1981); E.O. 12968 *Access to Classified Information* (Aug 4, 1995); PDD/NSC-12 *Security Awareness and Reporting of Foreign Contacts* (Aug 5, 1993); DCID 1/14 *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information* (Jan 22, 1992); DoD 5240.1-R *Procedures Governing the Activities of DoD Intelligence Components That Affect U.S. Persons* (Dec 82); DoD-2000.12 *DoD Combating Terrorism Program* (Sep 13, 1996); DoD-2000.14 *DoD Combating Terrorism Program Procedures* (Jun 15, 1994); and DoD-5240.6 *Counterintelligence Awareness and Briefing Program* (Jul 16, 1996). These policies are translated into various implementation policy directives and regulations (e.g., AFI 71-101 *Counterintelligence* [Jul 22, 1994]).

SCOPE

AFOSI is a worldwide field operating agency with headquarters in Washington, DC (Bolling Air Force Base). The agency has seven regional offices, plus seven overseas squadrons, and more than 160 subordinate detachments. These detachments have been empowered with considerable autonomy and run their own programs. Agents are located at all major Air Force installations and a variety of special operating locations. The organization is staffed by about 2,000 personnel, approximately two-thirds of whom are special agents. The vast majority of these career special agents (80%) are military personnel.

PROVIDERS' BACKGROUND AND TRAINING

All AFOSI agents have completed a 10.5 week basic course for special investigators at the U.S. Air Force Special Investigations Academy near Washington, DC, and are certified federal criminal investigators. Agents are assigned counterintelligence briefing responsibilities by their detachment commanders. Very little formalized training for presentations is available to them. The vast majority of counterintelligence briefing providers learn from experienced agents and through personal experience on the job.

PREPARATION FOR BRIEFINGS

Headquarters provides canned briefings to the detachments. As indicated above, these detachments exercise considerable autonomy, and can make use of these briefings as they see fit. Briefing providers indicated that they tailored their presentations to their local audiences and that they rarely relied on the canned briefings. Sources of background information used in preparing briefings included newspaper articles, security publications, and counterintelligence databases. Other personnel within AFOSI are also a major source of briefing material. External agencies that have provided useful information include CIA, DIA, DISA, DoDSI, DOE, FBI, NACIC, NRO, and NSA. Most providers felt that they had sufficient subject matter expertise to effectively communicate foreign intelligence threat information to Air Force audiences.

RECOMMENDATIONS

Persons interviewed in AFOSI offered a number of suggestions for improvements, e.g., briefings should be mandatory for all personnel. Both intra-agency and inter-agency information flow should be improved. Currently, the flow of information within AFOSI is primarily from the field up to Headquarters. Finally, there should be improved information flow among agencies (both DoD and non-DoD). Increased sharing of information (e.g., current threat information) would make the counterintelligence briefings more current, relevant, interesting, and effective.

Appendix F-2

AGENCY	ARMY 902D MILITARY INTELLIGENCE GROUP
HQ POINT OF CONTACT	Brian Lines Deputy for Operations

BACKGROUND

Located within the United States Army Intelligence and Security Command (INSCOM) is the 902d Military Intelligence (MI) Group whose mission is to protect the Army's forces, secrets, and technologies, by detecting, neutralizing and exploiting foreign intelligence services. Since the Cold War ended, targets have moved from Soviet/Eastern Block military plans, codes, and forces towards technology, the information superhighway, and nontraditional threats.

The 902d MI Group is comprised of a Headquarters and the 310th, 716th, and 308th MI Battalions, along with the Foreign Counterintelligence Activity which is responsible for offensive counterintelligence and the Central Security Facility which maintains the intelligence archives. With an overall budget of $27 million, the 902d operates in accord with policy guidance and oversight for security education from Headquarters DA, Office of the Deputy Chief of Staff for Intelligence. The 902d currently employs 417 civilians, 260 soldiers, 128 officers, and 90 warrant officers distributed across 37 offices in the US. The 308th MI Battalion has primary responsibility for supporting CONUS units by providing counterintelligence advice and assistance, conducting counterintelligence investigations and collections, and deploying tailored counterintelligence teams.

The Army 902d MI Group derives counterintelligence-related policy guidance from E.O. 12333 *US Intelligence Activities* (Dec 4, 1981); E.O. 12968 *Access to Classified Information* (Aug 4, 1995); PDD/NSC-12 *Security Awareness and Reporting of Foreign Contacts* (Aug 5, 1993); and DCID 1/14 *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information* (Jan 22, 1992). It is also guided by the major DoD directives, such as DoD 5240.1-R *Procedures Governing the Activities of DoD Intelligence Components That Affect US Persons* (Dec 1982); DoD-O-2000.12 *DoD Combating Terrorism Program* (Sept 13, 1996); DoD-O-2000.14 *DoD Combating Terrorism Program Procedures;* and DoD 5240.6 *Counterintelligence Awareness and Briefing Program* (Jul 16, 1996). These larger policies are translated into a number of smaller directives and regulations specifically designed for the Army. These include AR 381.12 *Subversion & Espionage Directed*

Against the US Army (SAEDA) (Jan 15, 1993); AR 380.5 *DA Information Security Program* (Feb 25, 1988); AR 381.47 *Counterespionage*; and AR 381-20 *US Army Counter Intelligence Activity* (Apr 17, 1987).

SCOPE

The Army 902d MI Group has one of the largest counterintelligence education and training programs in the Executive Branch. Counterintelligence information is disseminated by personnel at the 308th MI Battalion Headquarters, its two Military Detachments, and five Resident Offices located throughout the United States. Among these Resident Offices is the National Capital Region which is responsible for security education at DA Headquarters and in over 300 agencies and contractors in the Washington, DC area. Across the Army's 37 security offices are approximately 300 providers of security education and information.

Counterintelligence information in the Army is disseminated via two major vehicles: general awareness briefings and Counterintelligence Surveys. The Subversion and Espionage Directed Against the Department of the Army (SAEDA) general awareness briefings are unclassified and are designed to contact and educate large numbers of people with varied backgrounds. These briefings are presented annually by security managers in the field, utilizing and tailoring briefing materials supplied by the 902d. In FY 96, approximately 1,000 SAEDA briefings were presented to 96,000 people. In the future, SAEDA briefings will be given bi-annually and will be tailored to the highest risk groups, e.g., foreign travelers, those in contact with foreign visitors, scientists, etc.

Counterintelligence surveys are team assessments designed to produce leads and to provide commanders with information to help them target their counterintelligence program. This proactive and innovative program involves the use of a team of six to 20 interviewers who conduct structured one-on-one interviews with large numbers (150 - 250) of key personnel to determine the command's counterintelligence vulnerability in terms of its mission, expertise, and technologies. Owing its effectiveness in part to its top-down approach, the counterintelligence surveys are conducted only upon the request of the local commander. This approach has been successful in producing leads and systematic information which is added to DIA's database of which country/entity is interested in which technology and how they gather information. Approximately 40 counterintelligence are conducted each year.

In addition to the SAEDA and counterintelligence surveys, the 902d conducts terrorism briefings; classified nontraditional threat briefings tailored to the customer and related to its technologies, offices, mission, etc.; and travel briefings and debriefings.

PROVIDERS' BACKGROUND AND TRAINING

Ideally, the providers should have a minimum of 2 years experience in counterintelligence. Those with such experience include Officers in MOSs 35 E (CI) and 35D (MI); Warrant Officers in 351B (CI); Enlisted in 97B (CI); and Civilians in GS-132 (Intelligence), GS-134 (Intelligence and Assessments), and GS-080 (Physical Security). However, most of the 40 offices are run by Captains and junior officers who are assigned there for a year and do not have experience in counterintelligence; also, most Warrant Officers have tactical rather than strategic counterintelligence experience.

Providers are given some training on how to give presentations, but few receive training on how to generate effective leads. The Training Certification Program focuses on mechanics of presentation (e.g., military stage presence in terms of appearance, demeanor, presentation style). The Counterintelligence Survey Training Process trains the counterintelligence team members on issues related to the particular command being surveyed and its technologies, mission, and people. Also, some providers have attended the OPSEC Officer's Course. Overall, however, most of their expertise is gained via on-the-job experience.

PREPARATION FOR BRIEFINGS

The providers reported feeling relatively well prepared to design, develop, and present counterintelligence briefings. The 902d provides SAEDA and other briefing materials to be used at the local level. Most providers reported that they developed their own briefings utilizing the materials developed by the 902d and others, e.g., CIA, DIS, DoDSI, DOE, FBI, NACIC, NSA, and the Overseas Advisory Council. Other sources of useful information include newspaper articles, other parts of the organization, the Internet, security publications, books and articles on espionage cases, and databases. Most providers tailor their briefings for their audiences. Some use AR381-12 or DoD directives to establish specific learning objectives for their briefings; and some change the learning objectives for each presentation based on the type of audience, current issues, and the reason for the brief.

RECOMMENDATIONS

Persons interviewed within the Army 902d MI Group offered a number of recommendations for improvements to the counterintelligence program:

Measures of the effectiveness of the counterintelligence program in terms of its results should be developed, e.g., number and types of reports generated, whether the persons receiving the briefing or information use it.

The Executive Branch and each agency should make an institutional commitment to counterintelligence, emphasizing the word "counter" and linking counterintelligence policy directly with programs targeted. They should provide adequate DoD-level

counterintelligence training to teach the mechanics/process of security education and to ensure reporting results.

There needs to be a mechanism for sharing current security information across and within the different security education programs; e.g., on-line support in gathering counterintelligence information and materials, a central library of generic and agency-specific tapes and case information, especially dealing with nontraditional threat.

Appendix F-3

AGENCY	CENTRAL INTELLIGENCE AGENCY (CIA)
HQ POINTS OF CONTACT	Chief, Human Resources Management Staff Counterintelligence Center Chief, Awareness and Training Branch Office of Personnel Security

BACKGROUND

CIA has four main directorates--Operations, Intelligence, Administration, and Science & Technology.

FITA briefings are the responsibility of the Counterintelligence Center (CIC) in the Directorate of Operations, but there is little difference between counterintelligence and security awareness when the principal threat is insider betrayal. The Training Branch in the Office of Personnel Security (OPS) also gives a similar briefing to a different audience. CIC focuses more on existing employees while OPS focuses more on new personnel entering on duty. This division of labor appears to be effective.

CIA is guided by the same executive orders as other agencies plus a variety of internal CIA regulations regarding counterintelligence and security. No CIA regulation specifically mandates a periodic foreign threat awareness program. Given the unique nature of the CIA mission, security awareness and foreign threat awareness have always been part of the basic and specialized training programs and daily responsibilities of all CIA employees.

After the arrest of Aldrich Ames, the CIA Executive Director issued a classified memorandum establishing the Counterintelligence and Security Program (CISP). The CISP is a mandatory 4-hour briefng for all employees. It covers employees' accountability for their own actions, responsibility for reporting suitability and counterintelligence indicators that surface in a colleague's behavior, and an update on the foreign threat. The goal is to identify and then to either help or deal administratively with problem employees sooner. The original CISP program was defined in 1994 by a four-person committee of representatives from the Counterintelligence Center, Office of Personnel Security, Office of Medical Services, and Office of Training and Education.

SCOPE

CIC/Training has four full-time program managers, each responsible for a different set of courses. They do not conduct the briefings themselves. They arrange for subject matter experts from various other offices to give presentations. The program

managers determine the desired content, arrange for the presenters and monitor their performance, arrange for any handouts and audiovisual support, and handle all the administrative tasks connected with setting schedules, obtaining sites, and registering students.

CIC has the following training courses dealing with threat awareness: *Counterintelligence and Security Program, Overview of Critical Counterintelligence Issues for Intelligence Managers, CI Implications of Technological Advances, Field CI Seminar, CI Orientation,* and *Overseas CI Orientation.*

OPS/Awareness and Training Branch has four full-time providers. They handle the following courses dealing with threat awareness: *Introduction to CIA, Security Orientation Program* (several versions for different audiences), *Foreign Travel Briefing,* and *SCI Briefing.*

PROVIDERS' BACKGROUND AND TRAINING

The CIC/Training program managers all have some background in counterintelligence and/or operations. As noted above, they plan and manage the training courses but do not conduct the presentations themselves. With the exception of the CISP program, all presentations are given by subject matter experts. All the program managers are working toward qualification for certification as instructors by the CIA Office of Training and Education. This includes taking course work on teaching methodologies.

Owing to the considerable differences in perceptions and problems between the four main directorates, the CISP program is administered by directorate. The original CISP facilitators were designated by their directorate leadership to take on this task in addition to their regular duties. Although they went through a two-day training course to prepare them, few had any background in counterintelligence or security. This has evolved out over time so that there are now about 20 facilitators, all of whom are volunteers who believe in the program's importance and are quite adept at the job.

OPS providers are in the GS-11 to 13 grade range, and all have 10 to 15 years experience in a variety of security or counterintelligence functions.

PREPARATION FOR BRIEFINGS

CIA is itself the source of much threat awareness information, so most information used in briefings is internally generated. Products from other agencies are used when they meet a need. For example, the DoDSI video, *You Can Make a Difference*, is used in the CISP course. A State Department video has also been used occasionally.

Instructors in CIC courses are specialists in their field, not full-time providers. Since they are the experts, they need little additional preparation. The multiple facilitators who present the CISP program in each directorate develop their own presentations

following detailed guidance on the topics to be included. Consistency is provided by a standardized slide presentation with an outline of topics, a notebook of information including a number of suggested scripts, and guidance from the CIC course managers. A CIC course manager sits in on each presentation to provide quality control.

OPS providers use a common set of slides that outline the presentation. Within these parameters, each may use his or her own style or knowledge to develop the specific content under each topic. The providers often listen to each other's presentation, so the content tends to become quite similar.

RECOMMENDATIONS

Persons interviewed at CIA offered a number of suggestions for improvements in the counterintelligence program:

CIC believes that threat awareness briefings need to be made sufficiently interesting and relevant to people's jobs that people attend because they want to, not because they have to. Too many people are believed to approach mandatory training sessions with their ears half shut.

OPS believes security needs to do more to trumpet their successes, e.g., when they catch things in time to forestall major problems. Before putting more money into counterintelligence or security, people want proof that it is working and that more resources will make it work better. Security personnel need to be able to provide that proof.

For some audiences, CIA sees a need to do a better job of teaching people how to recognize a recruitment pitch.

CIA wants to develop better guidance for implementing need-to-know policies. Perceptions of need-to-know are believed to be different in each of the four main directorates.

Appendix F-4

AGENCY	COAST GUARD (USCG)
HQ POINT OF CONTACT	Ronald J. Seidman Director, Security and Risk Management

BACKGROUND

Operating within the Department of Transportation, the Coast Guard is the primary federal agency with maritime authority for the United States. The service's multi-mission approach permits a relatively small organization to respond to public needs in a wide variety of maritime activities and to shift emphasis on short notice when the need arises. Its main missions are Search and Rescue, Maritime Law Enforcement, Maritime Safety, Marine Environmental Protection, Aids to Navigation, Ice Breaking Operations and National Defense. To carry out these missions, the USCG employs 5,400 civilians, 43,000 active duty personnel and military reservists, and 25 to 40 contractors. All Coast Guard military personnel are required to maintain eligibility for a secret security clearance and approximately 30% of the force currently hold a clearance at the Secret or Top Secret level. Those Coast Guard personnel assigned to Intelligence duties have been granted access to Sensitive Compartmented Information (SCI). In addition to the active duty and reserve personnel, the Coast Guard grants clearance to 200 Coast Guard Auxilarists.

Located at the USCG Headquarters is the Office of Health and Safety. Within this Office is the Office of Safety, Security and Environmental Health whose Chief of Security Policy and Management is responsible for developing counterintelligence policy and for providing counterintelligence support to the Atlantic and Pacific Areas and their District Offices. Within the Atlantic and Pacific Areas are five to six Districts, each with a District Security Manager. Each District has a number of subordinate commands, each with a Command Security Officer who works with the Area and District Security Managers. In all, there are 11 Security Managers, 350 Command Security Officers (in all major units), and 600 to 650 Classified Material Control Officers.

The USCG derives counterintelligence-related policy guidance from E.O. 12333 *US Intelligence Activities* (Dec. 4, 1981); PDD/NSC-12 *Security Awareness and Reporting of Foreign Contacts* (Aug. 5, 1993); E.O. 12968 *Access to Classified Information* (Aug. 4, 1995); and DCID 1/14 *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information* (Jan 22, 1992). These larger policies are translated into a number of directives and regulations designed for the Department of Transportation and, in turn, into specific

USCG instructions such as COMDTINST M5528.1 *Security Awareness, Training, & Education (SATE) Program* (Aug 3, 1993) and COMDTINST M5510.21 *Information Security Program* (Aug 5, 1996).

SCOPE

Counterintelligence concerns are only a small part of Security Policy and Management at USCG. At the national level, the USCG deals primarily with combined issues of intelligence and National Defense. As an example of its emphasis on intelligence, Headquarters is building a central database for losses and compromises. As one deterrent, the Personnel Security Program focuses on investigating backgrounds which include unexplained affluence. While counterintelligence is not a major focus, the Security Policy and Management division is responsible for ensuring that briefings are conducted, as appropriate, throughout the USCG and for providing counterintelligence policy and guidance to the field via written instructions and materials. In turn, each level (i.e., Area, District, Unit/Command) is responsible for conducting briefings tailored to its unique vulnerabilities. Those who are most involved in drug enforcement deal with counterintelligence daily due to the fact that many foreign countries gather and exchange intelligence information with drug cartels and drug smugglers.

The USCG does provide general security awareness briefings to its employees. It provides unclassified newcomer or indoctrination briefings and annual refresher briefings that provide security-related information. It also provides unclassified defensive travel briefings and debriefings, as needed, for those going to and from foreign countries, especially those countries that are sympathetic to drug traffickers. They have published a *Foreign Threat to Coast Guard Travelers* brochure.These briefings are conducted by 11 Security Managers and 350 Command Security Officers and over 600 Classified Material Control Officers. The number and types of briefings are logged at the local level, but there is no centralized tracking of briefings for the USCG as a whole. Required briefings are outlined in the various COMDTINSTs and are checked as part of their semi-annual unit security evaluations.

PROVIDERS' BACKGROUND AND TRAINING

As previously mentioned, USCG providers at the local level are Security Managers, Command Security Officers and Classified Material Control Officers. These individuals typically have at least one year of experience in counterintelligence matters as well as experience in security. They may or may not have received training on making effective presentations; in fact, the providers interviewed reported that they only feel well prepared to design and give effective briefings to a small extent. They also reported that any training in how to effectively disseminate FITA information, especially concerning how to motivate people to report contacts and observations, would be welcomed.

PREPARATION FOR BRIEFINGS

For the most part, presenters rely on canned briefings developed by the USCG or the DoD. To some extent, they develop their own briefings tailored to their local target audience. Materials used to develop these presentations are obtained from newspaper articles, security publications, threat messages, training/briefing materials collected over time, and government-produced videos. Materials are also obtained from other intelligence, counterintelligence, or security managers within the USCG; and from DoDSI, the FBI, and the General Services Administration.

RECOMMENDATIONS

Persons interviewed within the USCG offered a number of recommendations for improvements in the FITA program:

Counterintelligence needs to become a national priority, with its definition expanded to include domestic as well as foreign threats and nontraditional as well as traditional threats from all sources. Given this priority, the executive orders and directives should specify what each agency must do in the area of counterintelligence (e.g., require all employees to attend an annual or bi-annual awareness briefing).

Emphasis should be placed on the value of unclassified information. Far too much time is spent focusing on classified information to the exclusion of sensitive, unclassified, but highly valuable, information. This means that the counterintelligence awareness programs should be expanded to reach all employees, not just those who possess clearances.

NACIC should be a clearing house, collecting information and materials from agencies and sharing it with others so that providers do not have to deal with multiple agencies. Such information should include a centralized list of counterintelligence-related executive orders and directives.

Generic scripts, suggested formats for briefings, and videos should be published for use by all agencies. These materials should emphasize the serious impact foreign intelligence successes can have on our nation's economic and technological health as well as on other national security capabilities.

Appendix F-5

AGENCY DEPARTMENT OF COMMERCE (DOC)

HQ POINT OF CONTACT Joseph J. Burns
Special Agent

BACKGROUND

The Department of Commerce, founded in 1906, is one of the smallest cabinet-level agencies. Its mission is to promote job creation, economic growth, sustainable development, and improved living standards for all Americans, by working in partnership with business, universities, communities, and workers. This partnership aims to promote U.S. competitiveness in the global marketplace, keep America competitive with cutting-edge science and technology and an unrivaled information base, and provide effective management and stewardship of our nation's resources and assets.

Given its focus on business and trade and its highly decentralized organizational structure, Commerce has been characterized by some as the closest to private industry in the federal government. It consists of 14 separate budget and Secretary-level offices, including the Bureau of Export Administration, Economics and Statistics Administration (including the Bureau of Census), International Trade Administration, National Oceanic and Atmospheric Administration, National Telecommunications and Information Administration, and Technology Administration. While they have many common goals, these diverse elements are operationally decentralized and have unique cultures, leadership, staffing and functional requirements. The over 35,000 Commerce employees vary considerably, with only 10-15 percent having clearances and many being scientists.

At Commerce, the Office of Security resides within the Office of the Chief Financial Officer and Assistant Secretary for Administration and is located at the Department Headquarters in Washington, DC. Headquarters Office of Security is responsible for establishing and providing threat awareness in counterintelligence-related matters to the various elements; thus, it serves but has no direct authority or operational control over the Security Officers who report directly to the element directors.

The Department of Commerce derives counterintelligence-related policy guidance from E.O. 12333 *US Intelligence Activities* (Dec. 4, 1981); E.O. 12968 *Access to Classified Information* (Aug 4, 1995); PDD/NSC-12 *Security Awareness and Reporting of Foreign Contacts* (Aug 5, 1993); and DCID 1/14 *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information* (Jan 22, 1992). These larger policies are translated into directives and regulations specifically designed for Commerce. A key departmental instruction is Com DAO 207-1

Department of Commerce Administrative Order (DAO) Personnel Security and Suitability Program which authorizes the development, issuance, and maintenance of a Security Manual that implements E.O. 10450, DCID 1/14, and PPD 12. Other instructions include CIAPS *Foreign Intelligence Recruitment Approaches* (Jan., 1996); *Defensive Travel Briefing* (1996); *Handling Classified and Sensitive Unclassified Information in the Scientific Community* (1996); and *Information Security Manual* (May 1996).

SCOPE

Headquarters Office of Security has established a modest, generalized counterintelligence awareness program. This program develops and provides briefings and supporting information to 30 to 50 element Security Officers who, in turn, are responsible for briefing element staff and contractors. It also provides counterintelligence-type briefings and materials to the Department and, upon request, to element administrations located in the Washington, DC, area. These briefings are presented by several providers within Headquarters Office of Security and by 15 to 20 providers located in the various elements. Within the larger elements there are three to 10 full-time providers; within the smaller elements there are two or fewer (sometimes no) part-time providers.

Threat awareness information is disseminated via newcomers briefings, national security information briefings, refresher briefings, information technology security briefings, classification management training, generic sensitive compartmented briefings, written generic foreign travel briefings and debriefings, and one-on-one travel briefings tailored to specific countries and audiences. In addition, there are special access briefings such as threat assessment of intelligence or terrorism in specific countries, NATO briefings, and COMSEC briefings. Headquarters Office of Security provides national security information briefings on a monthly basis to newly cleared employees, refresher briefings bi-annually, and travel briefings as needed. The frequency with which these and other briefings are adapted and given elsewhere varies depending upon the leadership and culture of each element. To supplement these oral briefings, Headquarters Office of Security provides generic written travel briefings, monthly security quizzes distributed via e-mail, and security awareness fairs and materials (e.g., posters, wallet reminders).

PROVIDERS' BACKGROUND AND TRAINING

Providers vary in terms of their experience. Some are special agents familiar with counterintelligence; others are administrative personnel who may not have prior counterintelligence knowledge or briefing skills. Generally, Security Officers enter their job with little experience and acquire knowledge and briefing skills on-the-job. Training received by providers includes courses given by DoDSI (e.g., DoD Security Briefer's

Course), Security Awareness and Education Subcommittee (SAES) Security Educators Seminars, and Train-the-Trainer Courses. While providers have been pleased with the quality of their training, they would like to attend courses to learn more effective ways to conduct threat awareness briefings.

Headquarters Office of Security hosts the annual DoDSI Strategies for Security Education Course and provides element Security Officers with information via e-mail about available training and seminars related to threat awareness and briefing skill development. Some elements provide specialized training for their own staff; for example, the National Oceanic and Atmospheric Administration hosts general awareness briefings using local police as experts.

PREPARATION FOR BRIEFINGS

The providers at headquarters reported being well prepared to design, develop, and present awareness presentations. These providers create briefings tailored to their audience by culling information from newspaper articles, security publications, and other parts of the organization. Their most useful source is the NACIC counterintelligence awareness network; but they also rely on the CIA, DoDSI, Energy, FBI, NRO, NSA, and the Overseas Advisory Council for information and materials. Specific country threat information, obtained from the State Department's classified system, is used to update Commerce's country files and to develop travel briefs. Providers within various elements receive information from headquarters via the *CI Digest* which contains examples of recent and relevant espionage cases. The extent to which this information is used or tailored to the elements is not known since there is no centralized tracking system.

RECOMMENDATIONS

Persons interviewed at Commerce offered a number of suggestions for improvements in the counterintelligence program:

NACIC should take a fresh look at the threat awareness process itself and develop a modern system to handle economic and other nontraditional types of espionage. This would involve moving from total protection to a risk management system.

Specific information should be available via INTELINK and other computerized databases, both classified and unclassified. These centrally maintained databases should include sources for different types of counterintelligence-related information, training opportunities for providers, and briefing experts and their availability.

Summary and specific information on the threat itself and how the threat is operationalized is needed. For example, what is the threat for different types of agencies, geographical locations, information or technologies; what are current methods (by country or organization) used to gather intelligence information; and where and how is terrorism being utilized and exploited.

Tracking of counterintelligence program activities and their effectiveness is needed. Currently, there is no way to tell if the information is reaching its targeted audience and, if it reaches the audience, if it is effective.

Appendix F-6

AGENCY	CUSTOMS SERVICE
HQ POINT OF CONTACT	Randy Greenstein Security Division Branch Chief

BACKGROUND

The Customs Service, one of the oldest agencies in the U.S. government, is the nation's principal border agency. Its mission is to ensure that all goods entering and exiting the United States do so in accordance with all United States laws and regulations. This mission includes enforcing U.S. laws interdicting narcotics and other contraband; protecting the American public and environment from the introduction of prohibited hazardous and noxious products; assessing and collecting revenues in the form of duties, taxes, and fees on imported merchandise; regulating the movement of persons, carriers, merchandise, and commodities between the U.S. and other nations while facilitating the movement of all legitimate cargo, carriers, travelers, and mail; interdicting narcotics and other contraband; and enforcing certain provisions of the export control laws of the U.S.

Operating within the Department of the Treasury, the Customs Service is headed by the Commissioner of Customs at the Service Headquarters in Washington, DC. At the Assistant Commissioner level is the Office of Investigations which, among other things, is responsible for carrying out threat assessments when Customs agents' lives are in danger. Within the Office of Investigations, the Intelligence Division develops policies and provides threat information received from overseas offices; and the Internal Affairs Division handles investigations and counterintelligence affairs within Customs.

The number of Customs employees at headquarters is few compared to the over 18,000 Customs employees who work in numerous field operations and focus on service delivery at ports of entry. These employees often have access to documents, data, and computerized systems containing very sensitive information. Although this information is most often classified as For Official Use Only (FOUO), it has tremendous value to others. For example, the Treasury Enforcement Communication System, one of the most complete systems within law enforcement, contains over 9,000 records of FOUO information; and other systems such as the Currency Transaction Reports, Currency Monetary Information Reports, and Title IV Database contain information on business organizations, bankers, economic information, drug trafficking, and the trade policies and products of other countries.

The Customs Service derives counterintelligence-related policy guidance from E.O. 12333 *US Intelligence Activities* (Dec 4, 1981); PDD/NSC-12 *Security Awareness and Reporting of Foreign Contacts* (Aug 5, 1993); E.O. 12968 *Access to Classified Information* (Aug 4, 1995); and DCID 1/14 *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information* (Jan 22, 1992). These larger policies are translated into directives and regulations specifically designed for the Department of the Treasury and, in turn, for the Customs Service. One such instructional manual within the Customs Service is the *Automated Information Systems (AIS) Security Policy Manual* that provides direction and guidance to protect AIS resources.

SCOPE

Customs does not have a counterintelligence-related or FITA program per se; rather, it has an awareness and integrity program that focuses on the integrity of its workforce and the prevention of potential bribes of Customs officals. Upon entry into the Customs Service, employees receive newcomers briefings. Those who are to become Customs officials attend the Federal Law Enforcement Training Center (FLETC) in Georgia where they receive career survival instruction covering basic bribery prevention and ethical decision-making training. Annually, thereafter, these officials attend a refresher bribery briefing. Those who are required to travel to foreign countries are provided with one-on-one travel briefs as needed. In addition, the Treasury Department provides briefings concerning the handling of classified materials for Customs employees cleared above the Secret level.

There are five Resident Area Customs (RAC) Offices throughout the United States, and each RAC is responsible for approximately 20 field locations. At the local units, the Resident Agents in Charge of the RACs and Special Agents in Charge (SAIC) of the field offices provide annual refresher bribery briefings and travel briefings as needed. Also, via Customs involvement in the Treasury Terrorist Advisory Group (TTAG), terrorist information is shared with employees as appropriate. In addition to these standard briefings, Customs communicates with industry via flyers and maintains an 800 number for reporting fraud and integrity issues. Customs does not have a centralized system to keep track of the number of these briefings that occur annually.

PROVIDERS' BACKGROUND AND TRAINING

When Customs agents serve on interagency teams, presenters from other agencies (e.g., FBI, State Department) provide threat awareness briefs and debriefs. Within Customs, the RACs and SAICs who provide the annual refresher bribery and travel briefings at the local level are current or former agents. Typically, these agents are hired from colleges, the military, private industry, and the intelligence community; and then are trained at FLETC and internally within Customs. Usually the providers are selected because they are available or they volunteer and learn to give effective briefings on the job, not via formal training.

PREPARATION FOR BRIEFINGS

In conjunction with FLETC, the U.S. Customs Service Office of Internal Affairs has produced a 40-minute videotape, *Play It Cagey 1 & 2*. Via this videotape and follow-up discussions, Customs officials are taught how to deal effectively with bribes. Internal Affairs also provides local units and industry with information such as security posters, the 800 number fraud and integrity issue hot line, and flyers. Some of these materials are developed in-house, but others are obtained from Liaison Officers working at Customs who bring in materials from other agencies.

RECOMMENDATIONS

Persons interviewed within the Customs Service offered a number of recommendations for improvements to the FITA program:

Top management in non-DoD agencies need to be convinced that there is a real threat to economic and technological information.

More attention should be paid to awareness training in terms of its content, the relevance of its content to specific agencies, and how its content is conveyed to target audiences. For example, a program should be created to make industry aware of the threat and of the need for technology and other types of control systems; and specific programs within non-DoD and DoD agencies should be assessed for security awareness purposes.

NACIC should serve as a clearing house for input and output, e.g., up-to-date standardized travel information. This would help ensure that there is a consistent and unified message concerning the threat and what to do under which circumstances.

Appendix F-7

AGENCY	DEFENSE INFORMATION SYSTEMS AGENCY (DISA)
HQ POINT OF CONTACT	Robert W. (Rob) Rogalski Chief of Security Security Division (D16)

BACKGROUND

DISA is the DoD agency responsible for information technology and is the central manager of major portions of the Defense Information Infrastructure (DII). DISA is responsible for planning, developing, and supporting Command, Control, Communications, Computers, and Intelligence (C4I) that serve the National Command Authority under all conditions of peace and war. DISA is subject to the direction, authority, guidance and control of Assistant Secretary of Defense (C3I) and responsible to the Chairman of the Joint Chiefs of Staff for operational matters. The agency's mission is to plan, engineer, develop, test, manage, acquire, implement, operate and maintain information systems for C4I and mission support under all conditions of peace and war.

DISA derives counterintelligence-related policy guidance from E.O. 12333 *U.S. Intelligence Activities* (Dec 4, 1981); E.O. 12958 *Classified National Security Information* (Apr 17, 1995); E.O. 12968 *Access to Classified Information* (Aug 4, 1995); PDD/NSC-12 *Security Awareness and Reporting of Foreign Contacts* (Aug 5, 1993); DCID 1/14 *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information* (Jan 22, 1992); DoD 5240.1-R *Procedures Governing the Activities of DoD Intelligence Components That Affect U.S. Persons* (Dec 82); DoD-2000.12 *DoD Combating Terrorism Program* (Sep 13, 1996); DoD-2000.14 *DoD Combating Terrorism Program Procedures* (Jun 15, 1994); and DoD-5240.6 *Counterintelligence Awareness and Briefing Program* (Jul 16, 1996). These policies are translated into various implementation policy directives and regulations. Two examples are: *Information Security Program* (DISA Instruction 240-110-8, Jun 1996) and *Desk Reference Guide to Executive Order 12958 Classified National Security Information*, DoDSI, DoD Edition).

SCOPE

DISA has over 9,500 employees worldwide. All these people have security clearances at the Secret level or higher. About 2,500 employees have SCI access. The organizational staff includes eight directorates: Personnel and Manpower (D1), C4 and Intelligence Programs (D2), Operations (D3), Logistics and Procurement (D4), Strategic Plans and Policy (D5), Engineering and Interoperability (D6), Joint Requirements Analysis and Integration (D7), and C4I Modeling, Simulation, and

Assessment (D8). DISA field and line organizations include: (1) DISA Western Hemisphere Theater (WESTHEM), (2) Defense Information Technology Contracting Office (DITCO), (3) Joint Interoperability Test Command (JITC), (4) Joint Interoperability and Engineering Organization (JIEO), (5) DISA Europe, and (6) DISA Pacific. There are field offices to support assigned Commanders in Chief and components. Finally, DISA has personnel in the National Communications System (NCS) and the White House Communications Agency (WHCA).

Security awareness responsibility is assigned to the Security Division (D16) of the Personnel and Manpower Directorate (D1). D1 is responsible for the component of the DISA that provides plans, programs and oversight worldwide in the mission areas of civilian personnel, military personnel, human resource development, executive services, manpower management, and security. In addition to worldwide responsibilities, the Deputy Director for Personnel and Manpower is responsible for providing direct service support for all DISA activities in the National Capital Region (NCR). Direct service support for DISA activities located outside the NCR is provided by non-DISA organizations under Host/Tenant Agreements or Inter/Intra Service Support Agreements. However, established DISA policy and oversight applies regardless of location.

Newcomer security awareness briefings are presented monthly by Security Division (D16) personnel. The following briefings are presented as needed: refresher briefings (at least one per year), travel briefings (required for all foreign travel), foreign visitor briefings for escort officers (about 40 per year), and termination briefings (presented to employees leaving DISA). A Memorandum of Understanding has been established between DISA and NCIS, authorizing NCIS to provide counterintelligence support to DISA. Based upon this interagency agreement, a special agent from NCIS has been assigned to DISA. This individual is responsible for presenting the counterintelligence-related briefings at DISA NCR locations and coordinating counterintelligence briefings at DISA field locations. In addition to briefings, security awareness is communicated by pamphlets, posters, the DISA Intranet, a Security Bulletin Board System (BBS), and a DISA Security Committee, chaired by the Chief of Security.

PROVIDERS' BACKGROUND AND TRAINING

The backgrounds of the personnel presenting security awareness briefings are quite varied. Some people have counterintelligence backgrounds (e.g., the NCIS agent), while others have little or no background in foreign intelligence threat awareness. For most of the security managers throughout DISA, the job is a part-time responsibility. A 5-day course, *Effective Briefing Techniques*, is sponsored by DISA and is available to employees. A significant part of the training is on the job, from experienced DISA personnel and via direct briefing experience.

PREPARATION FOR BRIEFINGS

As indicated above, the awareness briefings are presented by an NCIS special agent. In preparing for presentations, a good portion of the material is obtained from within DISA and NCIS. Other sources of information and materials include CIA, DIS, DoDSI, FBI, NACIC, and NSA. In each briefing, the topic of the foreign intelligence threat is introduced with information tailored to that specific audience. The central portion of all awareness briefings is a videotape entitled *Espionage: A Continuing Threat*. Upon completion of the videotape, the agent provides information on reporting procedures and answers any questions from the audience. Finally, the agent remains in the briefing room for a period to address any issues which audience members wish to discuss in private.

RECOMMENDATIONS

People interviewed in DISA offered a number of suggestions for improvements:

There should be an increased emphasis on communicating that security threats exist in employees' offices, not just on travel. This emphasis would be designed to counter the false sense of security felt by many employees in their DISA offices. The message would include the vulnerability of computer systems and networks to information compromise.

The counterintelligence community perspective should be changed so that being a foreign intelligence target is not considered a negative reflection on an agency. This would encourage disclosure and information sharing between agencies. An intranet system should be developed for security professionals to facilitate sharing information on targets, collection efforts, and lessons learned.

Appendix F-8

AGENCY	DEFENSE INTELLIGENCE AGENCY (DIA)
HQ POINT OF CONTACT	Margaret I. Obert Chief, Policy and Security Awareness

BACKGROUND

DIA is a combat support agency and the senior military intelligence component of the intelligence community. Established during the heightened Cold War tensions and impending crises in Berlin and Cuba in October 1961, DIA is the primary, all-source, multi-discipline intelligence arm of the Secretary of Defense and Chairman of the Joint Chiefs of Staff (CJCS), with responsibility to fulfill national-level missions and support the Combatant Commands of the U.S. Armed Forces. Intelligence support for operational forces encompasses a number of areas and challenges. Key areas of emphasis include warning of impending crisis, targeting and battle damage assessment, weapons proliferation, support to peacekeeping and Operations Other Than War, maintenance of databases on foreign military organizations and their equipment and, as necessary, support to U.N. operations and U.S. allies. In addition to providing timely and accurate intelligence to warfighters, DIA has other important customers, including decision and policymakers in the DoD and members of the Joint Chiefs of Staff. Additionally, DIA plays a key role in providing information on foreign weapons systems to U.S. weapons planners and the weapons acquisition community. In carrying out these missions, DIA coordinates and synthesizes military intelligence analysis for DoD officials, individual military services, and the U.S. Unified Commands.

DIA derives counterintelligence-related policy guidance from E.O. 12333 *U.S. Intelligence Activities* (Dec 4, 1981); E.O. 12958 *Classified National Security Information* (Apr 17, 1995); E.O. 12968 *Access to Classified Information* (Aug 4, 1995); PDD/NSC-12 *Security Awareness and Reporting of Foreign Contacts* (Aug 5, 1993); DCID 1/14 *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information* (Jan 22, 1992); DoD 5240.1-R *Procedures Governing the Activities of DoD Intelligence Components That Affect U.S. Persons* (Dec 82); DoD-2000.12 *DoD Combating Terrorism Program* (Sep 13, 1996); DoD-2000.14 *DoD Combating Terrorism Program Procedures* (Jun 15, 1994); and DoD-5240.6 *Counterintelligence Awareness and Briefing Program* (Jul 16, 1996). These policies are translated into various implementation policy directives and regulations. Two examples are the *Information Security Program* (Defense Intelligence Management Document, DIAR 50-2, Jul 15, 1993) and the *DIA Desk Reference Guide to Executive Order 12958 Classified National Security Information* (DoDSI and DIA, Oct 1995).

SCOPE

DIA is headed by a three-star flag officer. Personnel include both civilian employees and active duty military assignees from each of the military services, as well as reservists. These personnel work in several locations in and around the Washington, DC area. The majority of DIA employees work in the Defense Intelligence Analysis Center (DIAC), located on Bolling Air Force Base, the Pentagon and other nearby locations. Others work at the Armed Forces Medical Intelligence Center (Maryland) and the Missile and Space Intelligence Center (Alabama). Additionally, Defense attaches from DIA are assigned to U.S. embassies around the world. Finally, there are DIA liaison officers assigned to each Unified Command.

Responsibility for DIA security awareness and counterintelligence threat briefings is assigned to the Policy and Security Awareness Branch (DAC-2B) of the Security Division (DAC-2), within DIA's Counterintelligence and Security Activity (DAC). A variety of security briefings are presented to target audiences as needed. These include initial security orientation briefings for new personnel, quarterly security refresher training, defensive overseas travel security briefings, and counterintelligence threat briefings. Briefings are presented not only by DAC-2B personnel, but by a cadre of branch and division-level unit security officers (USOs) and special security contact officers (SSCOs). Posters and other security awareness materials are freely distributed throughout the agency to further enhance security awareness. Computer messages and advertisements are also used.

PROVIDERS' BACKGROUND AND TRAINING

Personnel are assigned to briefing responsibilities as needed. Some of these people have a civilian security background (GS-132 and GS-080) and/or a military security background. Guidance on conducting foreign intelligence awareness activities is provided by DoD 5200.1R, DoD 5240.6, DIAR 50-2, and DoDD 0-2000.12. In addition, courses by DoDSI and the Security Awareness and Education Subcommittee (SAES) of the Security Policy Board are available. People interviewed indicated that they felt well prepared to project professional credibility for foreign intelligence threat awareness, design effective presentations, speak before audiences (including senior level audiences), and keep audiences' attention.

PREPARATION FOR BRIEFINGS

DIA providers utilize a wide variety of materials for their presentations. Computer-based PowerPoint© briefings are the agency standard and are quickly replacing overheads and 35mm slides. Security awareness briefings conducted at DIA frequently utilize videotapes and supplemental reading materials for attendees such as brochures, pamphlets and other handouts. In preparing for briefings, providers obtain much of their information from within DIA. Other resources for current source information mentioned

in interviews with providers included the DoDSI, FBI, and NACIC, as well as such organizations as the American Society of Industrial Security and Overseas Security Advisory Council.

RECOMMENDATIONS

People interviewed in DIA offered their ideas for improvements. One suggestion was that efforts should be made to increase the information available on security problems encountered by private industry. In fact, security problems encountered by private industry are a primary concern of NACIC. In the past, corporations have been reluctant to divulge problems in this area for fear of not only upsetting stockholders, but jeopardizing lucrative government contracts.

Another suggestion was that a central repository of security information should be developed and made available to the security community. This would facilitate information-sharing among agencies, increase efficiency by reducing redundancy, and reduce the cost of information collection, materials development, and maintenance. DAC is currently working on a security home page on Internet, which will enable users to hyperlink to a variety of security-related categories, to include policy, threat, education, and reference library, among others. When completed, this should be far more effective than a repository.

Appendix F-9

AGENCY	DEFENSE INVESTIGATIVE SERVICE (DIS)
HQ POINT OF CONTACT	Gary L. Manning, Chief Counterintelligence Office

BACKGROUND

DIS is an agency of the DoD responsible for personnel security investigations; the administration of the Defense portion of the National Industrial Security Program; the Arms, Ammunition and Explosives Program; the Key Asset Protection Program; and Counterintelligence support. DIS reports that the creation of a counterintelligence support office within DIS has infused vitally important counterintelligence knowledge and experience into the DIS workforce.

Reinvention at DIS has steered the agency away from its former compliance mentality to the totally new approach of risk management. The DIS counterintelligence program was only recently established in response to this development. Under the new risk-management approach to security, the threat is more clearly defined and communicated in efforts to identify and manage the risks to defense contractors working on classified information.

The goal of the counterintelligence program at DIS is to educate the field force to collect counterintelligence information from intelligence sources and industry to make threat-appropriate, rational, and cost-effective decisions on managing the risk. A second goal is to provide information to the defense contractor community.

The DIS derives counterintelligence-related policy guidance from PDD/NSC-12 *Security Awareness and Reporting of Foreign Contacts* (Aug 5, 1993); and the National Industrial Security Program Operating Manual (NISPOM). In addition, guidance is provided by DIS Regulation 25-5 *Counterintelligence and Awareness Briefing Program*, April 23, 1987.

SCOPE

The counterintelligence program at DIS was established in 1995 with four personnel. Currently, there are 18 counterintelligence people at DIS. This includes three analyst positions provided by the Air Force, Army and Navy, and six Regional Counterintelligence Specialists posted throughout the country.

The audience of DIS's counterintelligence awareness program is targeted, for the most part, to its own personnel. This includes the 1,231 Special Agents (SAs) who perform personnel security investigations and the 211 Industrial Security Representatives (IS Reps) who facilitate implementation of security policies in defense contractor companies. DIS also attempts to provide threat awareness information to the defense contractor community through the Regional Counterintelligence Specialists and IS Reps.

The goal of the counterintelligence training for the SAs conducting personnel security investigations is to educate the workforce on current threats in the defense industry. This knowledge helps SAs recognize potential issues during the course of background investigations. The goal of the counterintelligence awareness program for the IS Reps is to teach what a threat assessment is, how to use it, and how to communicate it to the customer.

The backbone of the counterintelligence training for DIS employees revolves around what is called the Tools Course. This 4-day course explains potential espionage indicators, technology collection trends in the defense industry and cognitive interview techniques. Approximately 10 classes are held each year with 24 students in each class. The courses are taught by the DIS trainer with the two counterintelligence analysts providing specialist information. DIS personnel are also able to get threat information from the DISLINK-CI and STU-III bulletin boards. Training is provided by Regional CI Specialists as training facilities allow.

As mentioned above, additional training efforts are directed to Facility Security Officers (FSOs) at defense contractors who are responsible for implementing the security policies of the NISPOM. Regional CI Specialists and IS Reps may provide a threat briefing in any government-industry security education forum. Industrial Security Awareness Council (ISAC) meetings, for example, often provide an opportunity for a DIS threat briefing. The threat briefings are often based on a canned briefing developed by the counterintelligence office. The briefing reviews modus operandi of foreign intelligence services and current technology collection trends. The goal is to encourage FSOs to work with their IS Reps to gather specific threat information relevant to corporate operations. The National Industrial Security Bulletin Board (NISBB) for contractors also provides threat awareness information for the contractor community.

DIS is not an intelligence-gathering agency and does not have access to some of the more common sources of threat information. For example, limited funding inhibits access to all the intelligence databases. So DIS relies on other sources, including networking with professionals in the intelligence community. Yet the richest threat information comes from the customer base. DIS is in the unique position of visiting defense contractors on a regular basis during the security review process. And DIS has been fairly successful in collecting counterintelligence cases from the contractor community.

PROVIDERS' BACKGROUND AND TRAINING

The providers of threat information at DIS generally have personnel security investigator backgrounds; and some have a significant amount of counterintelligence experience. Many work closely with the DoDSI.

DIS uses information and courses from other agencies as much as possible. For example, DIS Counterintelligence Specialists are often trained by other agencies, such as the Joint Military Intelligence College, FBI, and DIA.

PREPARATION FOR BRIEFINGS

Most of DIS threat briefings follow a well-scripted lesson plan and briefing outline. Providers are able to insert relevant case examples depending on the audience and time available.

RECOMMENDATIONS

The people we interviewed at DIS would like to see increased coordination among government agencies and greater links to the intelligence community. In fact, DIS would greatly benefit from an FBI presence at the counterintelligence office because almost every counterintelligence case is referred to the FBI for information or action. Additionally, DIS counterintelligence personnel reported that they would like to have access to the intelligence databases to allow them to provide a better threat-appropriate product.

A number of additional recommendations for improvements to the program were offered:

Integrate counterintelligence awareness into their overall security operations as a support rather than operational function.

Provide faster access to sources of threat information from various sources. This may be accomplished by gaining access to secure intelligence databases. In addition, provide an environment conducive to working on classified information.

Continue to educate the DIS workforce on potential counterintelligence issues.

Provide more resources to allow for production of FITA material, new computers; provide field offices with access to secure bulletin boards; and allow DIS personnel to take more counterintelligence courses from other agencies.

Appendix F-10

AGENCY	DEPARTMENT OF DEFENSE SECURITY INSTITUTE (DoDSI)
HQ POINT OF CONTACT	Lynn F. Fischer Technical Publications Editor

BACKGROUND

DoDSI is tasked with training security professionals in a wide range of security disciplines; with the development and dissemination of publications and other educational products for security awareness enhancement; and, in general, with supporting security educational and briefing programs in the DoD and the defense contractor community. DoDSI's charter, DoD Directive 5200.32, February 1986, designates the Institute as the department's primary resource for security countermeasures education, training, and professional development support.

The Institute serves a customer base of nearly three million cleared personnel who handle 75 to 100 million classified documents, and provides security education and training to DoD military personnel and civilian employees, personnel of approximately 20 other federal agencies, and to federal contractor personnel. The Institute offers resident, field extension, teletraining, and independent study in support of a large number of defense and national security programs. The Institute graduates over 15,000 students annually through resident, on-site, customized, and independent study courses.

DoDSI receives policy direction, oversight, and technical guidance from the Principal Director, Information Warfare, Security, and Counterintelligence, in the Office of the Deputy Assistant Secretary of Defense (Intelligence and Security), Assistant Secretary of Defense (Command, Control, Communications and Intelligence), ASD (C3I). It continues to receive administrative support from the Defense Investigative Service (DIS) and the Defense Logistics Agency. Day-to-day management responsibilities for the Institute have been delegated to DIS.

The Institute also manages the activities of the Interagency Training Center (ITC), Training Activity, which provides technical surveillance countermeasures training for the entire federal law enforcement, security, and intelligence communities.

A significant part of DoDSI's mission is to train and prepare government security professionals and contractor security officers for keeping their respective employee populations aware and appropriately knowledgeable of the continuing threat to US classified and critical information. DoDSI courses normally include threat information and two courses, *Security Briefers Course* and *Strategies for Security Education*, provide

professionals with the methodology for effective delivery of threat information to employee audiences. Another course, *Espionage Then and Now*, provides an overview of counterintelligence, espionage modus operandi and motivations in order to explain the intelligence threat. Under a pending agreement with the Director, Counterintelligence and Investigations, the Institute would integrate additional relevant counterintelligence topical areas into security professional training and publish supporting materials.

In addition to professional training, DoDSI staff writers develop and disseminate products to enhance security and threat awareness programs. The most well-known DoDSI publication is the *Security Awareness Bulletin* which is provided to approximately 12,000 DoD security professionals and, through a subscription service, to other agencies and defense contractor facilities; it is also available online through the DoDSI web page. Feature articles frequently provide timely threat information. For example, a recent issue contained a case study of the Roderick Ramsay/Conrad Spy Ring espionage conspiracy.

The *Bulletin* provides a ready vehicle for disseminating counterintelligence and threat information and product announcements. The Institute also produces *Recent Espionage Cases*, an unclassified publication frequently used as a briefing handout that includes short summaries of all cases reported in the public media since 1975. *Recent Espionage Cases* is updated with the latest case developments annually.

For the past several years, DoDSI has funded and collaborated with the Intelligence Community Project Slammer in the production of the Countering Espionage video series. Products to date include *You can Make a Difference*, *It's not a Victimless Crime, On Becoming a Spy*, and *Profile of a Spy*. These videos, which are based on on-camera interviews with convicted espionage offenders and family members, promote the concept of concerned coworker support for personnel security programs. The next video in this series, *Damage to the Nation*, will focus on actual damage to national security and economic strength resulting from espionage.

All threat awareness products originating with DoDSI and many others which would support community briefing programs are described in the publication, *Announcement of Products and Resource* (updated at 6 month intervals). The *Announcement* provides specific information about sources and availability of videos, CBT briefing packages, publications, and other threat awareness resources useful for delivering this message to employee populations in government and industry. It is prepared in cooperation with the Security Awareness and Education Subcommittee (SAES) of the Training and Professional Development Subcommittee under the Security Policy Forum.

SCOPE

DoDSI does not provide security or threat awareness briefings directly to employee populations.

RECOMMENDATIONS

DoDSI would like to see NACIC expand the *National Counterintelligence Production Catalogue* to include additional descriptive information about threat awareness products and specific information about how they may be obtained (e.g., vendor, cost, full address, POC).

Appendix F-11

AGENCY	DEPARTMENT OF ENERGY (DOE)
HQ POINT OF CONTACT	Steven J. Brown Program Manager Policy, Administration and Training Counterintelligence Division Office of Energy Intelligence

BACKGROUND

DOE is a large federal agency whose history traces back to the Atomic Energy Commission and the Manhattan Project in the 1940s. Established as a cabinet-level department in 1977, DOE's mission is to contribute to the welfare of the Nation by providing the technical information and scientific and educational foundation for technology, policy, and institutional leadership necessary to achieve efficiency in energy use, diversity in energy sources, a more productive and competitive economy, improved environmental quality, and a secure national defense. Carrying out this mission are over 17,000 federal employees and over 120,000 contractors located across Headquarters, 10 operations/field offices, a multitude of field entities (e.g., site offices, special purpose offices, regional support offices), and 24 laboratories. Headquarters provides policy guidance and support to these relatively independent field units.

At DOE, the FITA program resides within the Office of the Under Secretary for National Security and Environmental Management Programs, Office of Nonproliferation and National Security. Separate from the Security Division is the Counterintelligence Division, a relatively new division that has an operating budget of about $6 million, with $5.5 million going to the field. Both the Security Office and the Counterintelligence Division have a role in ensuring that cleared employees and contractors are aware of the foreign intelligence threat and that unclassified, yet sensitive, information and technology are protected from unauthorized individuals.

DOE derives counterintelligence-related policy guidance from E.O. 12333 *US Intelligence Activities* (Dec 4, 1981); E.O. 12968 *Access to Classified Information* (Aug 4, 1995); PDD/NSC-12 *Security Awareness and Reporting of Foreign Contacts* (Aug 5, 1993); and DCID 1/14 *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information* (Jan 22, 1992). These larger policies are translated into a number of smaller directives and regulations specifically designed for the Department of Energy: *Counterintelligence Procedural Guide* (Nov 1995) and DOE 5670.3 *CI Program Order, Counterintelligence Program* (Sept 4, 1992).

SCOPE

In the DOE laboratories, many employees are highly educated and cleared scientists and nuclear specialists with access to classified technological and scientific information. These scientists are among the most vulnerable targets to foreign intelligence threat due to their interactions with the many foreign scientists who visit and work within the laboratories. In addition to these cleared personnel, large numbers of employees at Headquarters and in the field do not have clearances; yet they have access to sensitive or proprietary information targeted for economic espionage.

DOE's counterintelligence awareness program is defensive in nature, with its primary goal being to ensure that all cleared employees are aware of the foreign intelligence threat and report any contacts. Within the counterintelligence office at Headquarters, seven federal employees and seven contractors support and provide policy guidance to the field. Two of these federal employees are responsible for developing and presenting awareness briefings to DOE employees and contractors at Headquarters as well as to the field and other government agencies and contractors, upon request. These individuals also provide counterintelligence-related information and materials to the field counterintelligence program managers who are responsible for briefing local units.

Headquarters' counterintelligence personnel provide newcomers' briefings, foreign travel briefings, counterintelligence awareness briefings, and counterintelligence refresher briefings. One Headquarters' provider presents one-on-one and small group foreign travel and counterintelligence awareness briefs to upper-level management and to employees who travel to foreign countries. Another presents large group briefings called Defensive Information for Counter Espionage (DICE). The DICE presenter is well known throughout the intelligence community for his unique, humorous, and effective presentations to DOE Headquarters' personnel and to contractors and other government agencies upon request.

The counterintelligence office also provides materials (e.g., threat information, posters, reminders) to 10 federal employees and 40 contractors who are responsible for providing awareness briefings in the field. Among these materials is a generic desk-top briefing and quick reference tool called *1997 Safeguards and Security Awareness Refresher Briefing: A Computer-Based Briefing.* This software, developed by the Office of Safeguards and Security, is used by employees and contractors on a voluntary basis in place of, or in conjunction with, their annual refresher briefing.

Every cleared DOE employee and contractor receives travel briefings as needed, an initial awareness briefing, and an annual refresher briefing. According to the DOE central database, approximately 12,400 briefings were given in FY96 to over 69,000 employees and contractors. With the availability of the new computerized refresher brief, the number of counterintelligence awareness briefings is expected to increase in the future.

PROVIDERS' BACKGROUND AND TRAINING

DOE providers tend to have extensive counterintelligence backgrounds, with many being former military intelligence and counterintelligence officers. Thus, these individuals are expected to be able to present counterintelligence awareness and foreign travel briefings without formal training. Some of these providers, but not all, have attended formal training courses such as the Counterintelligence for Security Professionals (CISP) course that covers all aspects of their job including briefing skills. Headquarters counterintelligence representatives attend the annual Training and Resource Data Exchange (TRADE) meeting for the Security Training Special Interest Group so they can learn and share training opportunities with the field. Other providers have completed presentation skills courses, internal web page development courses, and NACIC counterintelligence seminars.

In addition to training its own personnel, DOE allows other government and contractor personnel to attend the CISP course and DICE briefings that are given at security association meetings, NACIC regional seminars, and at other government agencies (e.g., White House, DIA, DIS, State Department).

PREPARATION FOR BRIEFINGS

Most of the providers feel very well prepared to design, develop, and present FITA presentations. These providers develop briefings from scratch and incorporate information they receive from Headquarters and from other agencies. Materials are gathered from many different sources, including newspaper articles, DOE counterintelligence and other databases, security seminars, security publications, DOE-produced videos, and personal experiences. Contacts within DOE and other agencies also provide useful materials. These contacts come from CIA, DIS, DoDSI, FBI, NACIC, NSA, State, Overseas Advisory Council, nongovernment security organizations, National Classification Management Society (NCMS), Travel Risk Forecasting Company, and from liaison with members of the intelligence community. Using these materials, the presenters tailor their briefings to a great extent for their audiences.

RECOMMENDATIONS

Persons interviewed in DOE offered a number of recommendations for improvements in the FITA program:.

The awareness program needs greater support from senior government and contractor management. This emphasis, coupled with appropriate financial resources, would make the program much more effective.

There is a need for NACIC and the counterintelligence community to develop measures of awareness program effectiveness.

Recent threat information relevant to DOE facilities and sites (e.g., industrial and technological espionage) is needed. This includes analysis of espionage cases, lessons learned from these cases, plus unsuccessful espionage attempts.

Joint training and continuing educational opportunities for counterintelligence officers, crossing agency lines, would be valuable.

There is a need for more creative ways of disseminating information so that it is less costly in terms of employee time and program budget.

Appendix F-12

AGENCY	FEDERAL BUREAU OF INVESTIGATION (FBI)
HQ POINTS OF CONTACT	Larry V. Watson National ANSIR Program Manager Bradley B. Benson Chief, Information Systems Security Jonathan P. Binnie Chief, National Security Training

BACKGROUND

The FBI is the principal investigative arm of the U.S. Department of Justice. It investigates those activities that violate federal laws or jeopardize the national security in areas that include espionage, counterterrorism, economic espionage (theft of trade secrets), and both physical and cyber infrastructures.

As the country's lead counterintelligence agency for the domestic, civilian population, the FBI is responsible for detecting and countering actions of foreign intelligence services (FIS). The theft of U.S. technology and sensitive economic information by FISs and their operatives has been estimated by the White House and others to be valued up to a hundred billion dollars each year. It is, therefore, prudent and necessary that the FBI provides information to those who are the targets of this activity.

FBI derives counterintelligence-related policy guidance from E.O. 12333 *U.S. Intelligence Activities* (Dec 4, 1981); Attorney General Guidelines, and various federal statutes. Personnel security-related guidance derives from E.O. 12356 (Apr 2, 1982); E.O. 12598 *Classified National Security Information* (Apr 17, 1995); NSD 197 (Nov 1, 1985); NSD 47; DCID 1/14 *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information* (Jan 22, 1992); 28 CFR Part 17; DOJ Order 2600.2B *Security Program and Responsibilities* (July 10, 1989); DOJ Order 2640.2C *Telecommunications and Automated Information Systems Security* (June 25, 1993).

SCOPE

The FBI has two separate foreign intelligence threat awareness programs: one for educating U.S. corporations, other government agencies and educational institutions, and another for FBI employees. The former is known as the Awareness of National Security

Issues and Response (ANSIR) program and is part of the FBI's National Security Division Operational Training Unit; the latter is the Security Education Program under the National Security Division Information Systems Security Unit.

The FBI's ANSIR Program is the public voice for espionage, counterintelligence, counterterrorism, economic espionage, cyber and physical infrastructure protection, and all national security issues. The program is designed to provide unclassified national security threat and warning information to U.S. corporate security directors and executives, law enforcement, and other government agencies. It also focuses on the response capability unique to the FBI's jurisdiction in both law enforcement and counterintelligence investigations.

Currently, information is disseminated nationwide via the ANSIR-FAX network. Each of the FBI's 56 field offices has an ANSIR Coordinator and is equipped to provide national security threat and awareness information, on at least a monthly basis, to as many as 500 recipients. ANSIR-FAX is the first initiative by the U.S. government to provide this type of information to as many as 25,000 individual U.S. corporations who have critical technologies or sensitive economic information that are targeted by FISs or their agents.

Beginning in August, 1997, the ANSIR Program launched the next level of communication via ANSIR-Email which, when fully implemented, will expand the number of recipients of unclassified threat and warning information to over 100,000. Through the use of the Internet, ANSIR Coordinators will have interactive Email capability with the majority of U.S. corporate security directors and others within their field divisions.

ANSIR-NET provides an overview of the ANSIR Program on the FBI's Internet home page located at: http//www.fbi.gov.

The FBI's Security Education Program is staffed at FBI Headquarters by two persons full-time and one other part-time. Each of the 12 FBI Headquarters divisions is staffed by a Security Officer as well as each section of those divisions. In the field, there is a Special Agent Security Officer in each of the FBI's 56 field offices. With appropriate FBI Headquarters guidance, the Security Officers are responsible for conducting periodic security awareness briefings for all FBI employees. These individuals also provide singular security briefings for specific individual employees which are triggered by a variety of factors such as foreign travel.

All new FBI employees receive information on the foreign intelligence threat during their initial indoctrination. New Special Agents are additionally provided a broader familiarization with the foreign intelligence threat during 3 days of their 16-week New Agent Training Program. This familiarization advises which foreign powers pose the greatest threat, how they operate, and what the FBI does to counter that threat. If the Special Agents become assigned to national security matters, they are provided intensive

counterintelligence training on a wide variety of subjects. The FBI mandates interactive, distance-learning training for its Special Agents upon assignment to national security matters.

PROVIDERS' BACKGROUND AND TRAINING

FBI ANSIR Coordinators are selected by the Special Agent in Charge (SAC) of the local field office. Criteria for selection include experience in national security investigations, advanced counterintelligence and counterterrorism training, computer literacy, and the ability to communicate effectively with others. ANSIR Coordinators meet regularly with industry leaders and security directors for updates on current national security issues. Annual in-service training conducted by the National Program Manager ensures that a consistent message for the ANSIR Program is maintained.

FBI Security Officers have similar backgrounds and are provided similar training. Security Officer training, however, includes special security administrative education in addition to threat awareness training.

BRIEFINGS

Although the primary method of communication between the FBI and industry is through electronic media, ANSIR Coordinators will, on occasion, conduct briefings to individuals or groups. Information is provided to corporations by the FBI to help them protect against theft of their technology. The ANSIR Program focuses on the techniques of espionage when relating national security awareness information to industry. Discussing techniques allows ANSIR Coordinators to be very specific in giving industry representatives tangible information to help them determine their own vulnerabilities. Through the ANSIR Program and the discussion of techniques of espionage, corporations are able to learn from the experiences of others and, hopefully, be able to avoid adverse results.

Along with awareness, the ANSIR Program focuses on the FBI's unique response capability with regard to issues of national security. The FBI has primary jurisdiction for a variety of criminal and counterintelligence matters which impact on national security. For instance, the recent passage of the Economic Espionage Act of 1996 opens up new areas for FBI response to the wrongful acquisition of intellectual property. It also encourages corporations to consider how best to protect their proprietary information or trade secrets from both domestic and foreign theft.

RECOMMENDATIONS

People interviewed at FBI offered the following recommendation: It is recognized that other federal agencies have developed awareness programs for the purpose of educating employees about the threat from FIS as well as domestic acquisition of economic espionage. A necessary element, however, of these awareness programs

must be to include information of the FBI's singular responsibility in matters of national security. Awareness coordinators of all federal agencies should feel free to include local ANSIR Coordinators in briefings of their personnel to ensure that employees are given specific information regarding the FBI's response capability.

Appendix F-13

AGENCY	FEDERAL EMERGENCY MANAGEMENT AGENCY (FEMA)
HQ POINT OF CONTACT	Jerry L. Prince Security Specialist (Operations)

BACKGROUND

FEMA is the federal government agency responsible for constructing and maintaining the emergency management system for the nation. The mission of FEMA is to provide leadership and support to reduce the loss of life and property and protect our nation's institutions from all types of hazards through a comprehensive, risk-based, all-hazards emergency management program of mitigation, preparedness, response, and recovery. The federal government provides resources grouped into 12 Emergency Support Functions (ESFs). FEMA has the Lead Agency responsibility for two of these: (1) ESF 5: Information and Planning--collecting, analyzing, and disseminating critical information to facilitate the overall federal response and recovery operations, and (2) ESF 9: Urban Search and Rescue--locating, extricating and providing initial medical treatment to victims trapped in collapsed structures.

FEMA derives counterintelligence-related policy guidance from E.O. 12333 *U.S. Intelligence Activities* (Dec 4, 1981); E.O. 12968 *Access to Classified Information* (Aug 4, 1995); PDD/NSC-12 *Security Awareness and Reporting of Foreign Contacts* (Aug 5, 1993); and DCID 1/14 *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information* (Jan 22, 1992). Policy guidance is also contained in FEMA documents (e.g., *Strategic Plan: Federal Emergency Management Agency*, Dec 1994).

SCOPE

FEMA headquarters is located in Washington, DC. Other organizational components include ten regional offices, area offices in Hawaii and the Caribbean, the Mt. Weather Emergency Assistance Center (Berryville, VA), and the National Emergency Training Center (Emmitsburg, MD). There are more than 2,600 full-time employees and nearly 4,000 standby employees who are available for service when disasters occur.

Foreign intelligence threat briefings are presented weekly to upper management personnel at headquarters. However, due to limited resources, this information is not presented to other employees. Security refresher briefings are no longer given. Newcomer briefings have also been discontinued; however, the Human Resources Management Office plans to create a newcomer information packet for new employees. Travel

briefings are presented on a one-on-one basis. There are three people who present security briefings at Headquarters, two at Mt. Weather, one at the National Emergency Training Center, and one provider at each of the ten regions.

PROVIDERS' BACKGROUND AND TRAINING

People providing security briefings at Headquarters all have counterintelligence-related backgrounds. In the regions, security personnel have backgrounds in intelligence and counterintelligence. Most have some military experience in these areas. Some of the providers have completed briefing courses. However, a significant degree of training is received on the job through direct briefing experience.

PREPARATION FOR BRIEFINGS

Headquarters provides briefing materials to the regions and centers. Some briefing materials are obtained from DoDSI. Brochures on various countries are obtained from the State Department for use in travel briefings. In addition, overheads, videos, and posters are used. At one point, FEMA had a contractor engaged in the development of briefing materials. However, budget cutbacks eliminated this resource. In some cases, guests from other agencies (e.g., CIA, DIA, and FBI) have conducted briefings for FEMA personnel.

RECOMMENDATIONS

People interviewed in FEMA offered the suggestion that a new executive order should be issued requiring an annual FITA briefing for everyone who has a security clearance.

Appendix F-14

AGENCY	JOINT STAFF (JS)
HQ POINT OF CONTACT	David G. Lippert Security Specialist Information Resources Management Office

BACKGROUND

The Joint Staff supports the Chairman and Vice Chairman of the Joint Chiefs of Staff and employs some 1,500 people, many of whom are senior members of the military (05s and above) and senior civilians. The Joint Staff provide military and national security advice to the National Command Authority; develop U.S. Joint/Combined military policy, strategy and doctrine; recommend military resource allocation; and plan and resource Joint/Combined operations. There are eight elements to the organization, each with a security manager. For purposes of this study we concerned ourselves only with the J2, Directorate for Intelligence (staffed by DIA), and the J3, Directorate for Operations.

Joint Staff employees deal with highly sensitive information, so they are particularly attractive to targeting by foreign intelligence and security services, not only when traveling abroad, but also within the US.

The Joint Staff derives counterintelligence-related policy guidance for its counterintelligence program from E.O. 12333 *U.S. Intelligence Activities* (Dec 4, 1981); PDD/NSC-12 *Security Awareness and Reporting for Foreign Contacts* (Aug 5, 1993); E.O. 12958 *Classified National Security Information* (Apr 17, 1995); *Information Security Oversight Office; Classified National Security Information; Final Rule* (Oct 13, 1995); E.O. 12968 *Access to Classified Information* (Aug 4, 1995); DCID 1/7-1 *Security Controls on the Dissemination of Intelligence Information* (Jun 15, 1996); DCID 1/14 *Personnel Security Standards and Procedures Governing Eligibility for Access to SCI* (Jan 22, 1992); DoD Directive 5200.1R *Information Security Program* (Jan 17, 1997); and DoD Directive 5240.6 *Counterintelligence Awareness and Briefing Program* (Jul 16, 1996).

SCOPE

The J2 has about 400 people, all DIA employees; the J3 has approximately 450-500. About a third of the military employees rotate each year so there is a great deal of turnover. There are about 250 permanent employees on the Joint Staff as a whole.

Security at the Joint Staff is divided into two major areas, Information Resources Management Office and the Security Office. The Information Resources Management Office covers information and automation security while the Security Office controls personnel and physical security. The Security Office does not include foreign intelligence threat awareness in their briefings, but it does conduct travel briefings.

J2 employees are briefed from time to time by their home agency, DIA. The Joint Staff as a whole is supported for foreign intelligence threat awareness by the Department of Energy's Defensive Information to Counter Espionage (DICE) program. The goal of the DICE program is to make sure employees are truly aware of the foreign intelligence threat and that they should report suspicious activity. Attendance at this program is mandatory once a year. If people cannot attend, they are given a videotape of the briefing.

All newcomers to the Joint Staff get several initial briefings from the Personnel Security Section of the Security Office. Under the recently initiated Joint Staff Training Program, newcomers receive a series of detailed briefings by Physical, Information, and Automated Information security experts from the Information Systems Security Division, Information Resource Management Office. In addition, the JS Information Security Manager briefs all new Directorate Security Managers. Directorate Security Managers then conduct security training for their Directorate personnel on a regular basis. All JS personnel receive the yearly DICE briefing.

As an additional part of the general awareness program at the Joint Staff, a monthly newsletter is published to provide security education and awareness on relevant security issues in all four security disciplines and keeps Joint Staff personnel up to date on all security mandates. The Joint Staff has its own homepage where security information can be highlighted. Posters published by the American Forces Information Services are distributed and there is a small library of videos, primarily from DIA, Navy and DoDSI, which are handed out to people if they have missed live briefings. New products are obtained when experts attend various seminars and meetings.

PROVIDERS' BACKGROUND AND TRAINING

See DOE and DIA profiles for provider training information.

PREPARATION FOR BRIEFINGS

Also see DOE and DIA.

RECOMMENDATIONS

People interviewed at the Joint Staff recommended the development of a centralized video program, with segments tailored to the various audiences in the government.

Appendix F-15

AGENCY	DEPARTMENT OF JUSTICE (DOJ)
HQ POINT OF CONTACT	James Fradel Assistant Director Information Security Policy

BACKGROUND

As "the largest law firm in the nation," the Department of Justice serves as counsel for its citizens. It represents them in enforcing the law in the public interest. Through its thousands of lawyers, investigators, and agents, the Department plays the key role in protection against criminals and subversion, in ensuring healthy competition of business in our free enterprise system, in safeguarding the consumer, and in enforcing drug, immigration, and naturalization laws. The Department also plays a significant role in protecting citizens through its efforts for effective law enforcement, crime prevention, crime detection, and prosecution and rehabilitation of offenders.

The Department's mission is to enforce the law and defend the interests of the United States according to the law, provide federal leadership in preventing and controlling crime, seek just punishment for those guilty of unlawful behavior, administer the nation's immigration laws fairly and effectively, and ensure fair and impartial administration of justice for all Americans.

DOJ derives counterintelligence-related policy guidance from E.O. 12333 *U.S. Intelligence Activities* (Dec 4, 1981); E.O. 12958 *Classified National Security Information* (Apr 17, 1995); E.O. 12968 *Access to Classified Information* (Aug 4, 1995); PDD/NSC-12 *Security Awareness and Reporting of Foreign Contacts* (Aug 5, 1993); DCID 1/14 *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information* (Jan 22, 1992); and 28 CFR Part 17 *National Security Information Program* (Nov 7, 1985). These policies are translated into various implementation policy directives and regulations (e.g., *Classified National Security Information*, DOJ, Mar 5, 1996 and *Classified National Security Information Marking Guide*, DOJ, May 28, 1996).

SCOPE

The Attorney General leads the Department of Justice, a key Executive Branch arm composed of more than 30 component organizations. These include five major bureaus for law enforcement: the Bureau of Prisons (BOP), the Drug Enforcement Administration (DEA), the Federal Bureau of Investigation (FBI), the Immigration and Naturalization Service (INS), and the United States Marshals Service (USMS).

While DOJ headquarters are located in Washington, DC, the majority of its work takes place elsewhere. Most of the total workforce (approximately 106,000 employees) are located in about 2,000 installations around the country, or in one of the approximately 100 overseas offices.

Unclassified briefings on National Security Information (NSI), and classified briefings on Sensitive Compartmented Information (SCI) are presented biweekly in Washington. New employees attend the NSI briefing. Refresher briefings are presented as requested. For most employees, travel briefings are only required for foreign travel. However, travel briefings for all travel are mandatory for personnel holding positions requiring SCI access.

PROVIDERS' BACKGROUND AND TRAINING

Many of the people responsible for presenting security briefings have a Security Specialist (GS-080) background.There are opportunities to attend training courses (e.g, Security Educators Seminar and a security briefers course). However, a significant portion of training takes place on the job, both from other DOJ personnel and by actual presentation experience.

PREPARATION FOR BRIEFINGS

In preparing for briefings, providers obtain much of their information from others within DOJ. Other sources of information include DoD, DoDSI, FBI, NRO, NSA, and the Overseas Advisory Council of the State Department. Providers feel reasonably well prepared to design effective presentations and to develop printed materials, and well prepared to speak before an audience and hold their attention.

Security briefings are augmented by handouts, newsletters, posters, and a computer-based training program, *National Security Information and You.* This training program was written in PowerPoint© by the Information Security Policy Group of the Security and Emergency Planning Staff.

RECOMMENDATIONS

People interviewed in DOJ offered a number of suggestions for improvements. Security issues should be addressed proactively by investing in preventative measures. At present, resources are usually received in reaction to a security problem (e.g., after the bombing of the Oklahoma City federal building).

Foreign intelligence threat awareness should place increased focus on the critical nature of technical information with high economic value, emphasizing that even friendly countries are conducting economic espionage against the U.S.

The availability of information on detected espionage should be improved. This may require the release of some "closely held information" to disseminate information that will enhance deterrence. Increased effort should be devoted to accurately describing the damage done by spies and delineating lessons learned from case files.

Appendix F-16

AGENCY	MARINE CORPS (USMC)
HQ POINT OF CONTACT	GYSGT Edward C. Krattli Counterintelligence Chief Human Intelligence Branch

BACKGROUND

Marine Corps Intelligence provides services and specialized products to support the Commandant of the Marine Corps as a member of the Joint Chiefs of Staff, as well as to the Marine Corps Headquarters Staff. Marine Intelligence supports acquisition policy and budget planning and programming, and provides pre-deployment training and force contingency planning for requirements that are not satisfied by theater, other service, or national capabilities.

Within the DON, the NCIS has the primary counterintelligence jurisdiction for noncombat matters and the responsibility for the execution and implementation of DON counterintelligence programs and policies. During combat, operations other than war, contingencies and deployments, the Marine Commander is responsible for, and exercises control over, all Marine Corps counterintelligence assets and operations. Additionally, Marine Corps counterintelligence personnel are assigned to various NCIS field offices and may augment NCIS to assist in specific investigations and operations.

USMC derives counterintelligence-related policy guidance from E.O. 12333 *U.S. Intelligence Activities* (Dec 4, 1981); E.O. 12968 *Access to Classified Information* (Aug 4, 1995); PDD/NSC-12 *Security Awareness and Reporting of Foreign Contacts* (Aug 5, 1993); DCID 1/14 *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information* (Jan 22, 1992); DoD 5240.1-R *Procedures Governing the Activities of DoD Intelligence Components That Affect U.S. Persons* (Dec 82); DoD-2000.12 *DoD Combating Terrorism Program* (Sep 13, 1996); DoD-2000.14 *DoD Combating Terrorism Program Procedures* (Jun 15, 1994); and DoD-5240.6 *Counterintelligence Awareness and Briefing Program* (Jul 16, 1996). These policies are translated into various implementation policy directives and regulations, including SECNAVINST 3875.1 *Counterintelligence and Awareness Briefing Program* (Nov 2, 1988) and OPNAVINST 5510.1H *Department of the Navy Information and Personnel Security Program Regulation* (Apr 29, 1988).

SCOPE

At Headquarters Marine Corps (HQMC) foreign intelligence threat information is included in overall security briefings. These monthly briefings serve as both an initial indoctrination briefing for newcomers and as a security refresher briefing for experienced personnel, both military and civilian. The security and terrorism briefings are presented by HQMC personnel; an NCIS representative presents the counterintelligence briefing. Travel briefings and special presentations on foreign intelligence threat and terrorism are made to individuals or small groups as needed at HQMC. SCI briefings are given to personnel requiring the information, as needed, usually in a one-on-one mode. At Marine commands, security briefings are presented by the unit's security manager. When requested, Marine Corps counterintelligence personnel and NCIS provide briefs on foreign intelligence threats to Marine commands.

PROVIDERS' BACKGROUND AND TRAINING

Although some briefing providers have attended formal training in relevant courses (e.g., security, terrorism, and counterintelligence), they receive a significant portion of their training on the job, both from experienced personnel at HQMC and by actual presentation experience. They feel that they have sufficient subject matter expertise to effectively communicate the required information. For additional information on the background and training of briefing providers, see the NCIS agency summary report.

PREPARATION FOR BRIEFINGS

In preparing for briefings, the presenters draw upon a number of sources of information. Two major sources are HQMC personnel involved in security and counterintelligence and NCIS. Other information sources used include CIA, DoDSI, FBI, NACIC, NRO, and NSA. For additional information on briefing preparation, see the NCIS agency summary report.

RECOMMENDATIONS

Persons interviewed in HQMC offered a number of suggestions for improvements. Increasing the availability of current foreign intelligence awareness information would be a significant improvement. At present, much of the information available is outdated. Other information, while more current, has restrictions on its use. Adherence to strict guidelines during the application and assignment of restrictions (e.g., ORCON) would improve the availability of counterintelligence information and make briefings more current, relevant, interesting, and effective.

A comprehensive catalog of materials available would facilitate resource sharing within the counterintelligence community. This catalog should include a description of the material content, information on availability, and a point of contact for additional information.

Appendix F-17

AGENCY	NATIONAL AERONAUTICS AND SPACE ADMINISTRATION (NASA)
HQ POINT OF CONTACT	Robert E. Turner Program Security Manager

BACKGROUND

NASA was established by the National Aeronautics and Space Act of 1958. This "Space Act" directed NASA to conduct space activities for peaceful purposes and for the benefit of all humankind, maintain the leadership position of the United States in aeronautics and space science and technology, expand the knowledge base on both the Earth and in space, conduct human activities in space, encourage commercial use of space, cooperate with other nations, and communicate scientific findings widely.

The agency's mission statement includes three objectives: to advance and communicate scientific knowledge and understanding of the Earth, the solar system, and the universe and use the environment of space for research; to explore, use, and enable the development of space for human enterprise; and to research, develop, verify, and transfer advanced aeronautics, space, and related technologies.

As indicated above, the agency's mission and objectives place a heavy emphasis on the dissemination of research findings. Its organizational emphasis on open communication and sharing of information makes the job of counterintelligence and security especially difficult. Scientists are concerned with conducting research and then communicating the results to their professional colleagues. Effectively delivering a message that emphasizes the need for security of information in this organizational environment is difficult and challenging.

NASA is organized into a Headquarters, located in Washington, DC, and 10 Centers of Excellence located around the United States. Each of these Centers has an established area of excellence and a specific mission: (1) Ames Research Center, Moffett Field, CA (Information Technology); (2) Dryden Flight Research Center, Edwards, CA (Atmospheric Flight Operations); (3) Goddard Space Flight Center, Greenbelt, MD (Scientific Research); (4) Jet Propulsion Laboratory, Pasadena, CA (Deep Space Systems); (5) Johnson Space Center, Houston, TX (Human Operations in Space); (6) Kennedy Space Center, Cape Canaveral, FL (Launch and Cargo Processing Systems); (7) Langley Research Center, Hampton, VA (Structures and Materials); (8) Lewis Research Center, Cleveland, OH (Turbomachinery); (9) Marshall Space Flight Center, Huntsville, AL (Space Propulsion); and (10) Stennis Space Center, SSC, MS (Propulsion Testing Systems). This extensive decentralization provides additional challenges to security personnel.

With some other agencies such as Commerce and Transportation, NASA is now involved with an Executive Agent program with NACIC that provides analytical counterintelligence support.

NASA derives counterintelligence-related policy guidance from E.O. 12333 *U.S. Intelligence Activities* (Dec 4, 1981); E.O. 12968 *Access to Classified Information* (Aug 4, 1995); PDD/NSC-12 *Security Awareness and Reporting of Foreign Contacts* (Aug 5, 1993); DCID 1/14 *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information* (Jan 22, 1992); DoD 5240.1-R *Procedures Governing the Activities of DoD Intelligence Components That Affect U.S. Persons* (Dec 82); DoD-2000.12 *DoD Combating Terrorism Program* (Sep 13, 1996); DoD-2000.14 *DoD Combating Terrorism Program Procedures* (Jun 15, 1994); and DoD-5240.6 *Counterintelligence Awareness and Briefing Program* (Jul 16, 1996). These policies are translated into various implementation policy directives and regulations covering NASA as a whole (e.g., *NASA Security Handbook* 1620.3C [Feb 1993]). The field installations translate this overall NASA guidance into specific implementation policies (e.g., Goddard Space Flight Center Security Office: *Security Manual* GHB 1600.1A [Nov 30, 1990]).

SCOPE

NASA has a small security threat awareness program which is very decentralized. Headquarters has two individuals who present information on all types of security matters, including initial security indoctrination briefings, security refresher briefings, foreign intelligence threat awareness briefings, and foreign travel briefings. Audiences for briefings include in-house personnel and on-site contractors. Each field installation has been empowered with a great deal of autonomy and discretion over the contents of its program. The reduction in security personnel resulting from downsizing has constrained the security programs at both Headquarters and the field installations.

PROVIDERS' BACKGROUND AND TRAINING

Historically, the security personnel at headquarters have had limited counterintelligence investigative experience. Problem identification has not been proactive, however. Current efforts are addressing these issues. People are assigned to the job on an "as-needed" basis. They have access to government courses, but there is no formalized, structured training plan. Briefing skills are largely developed and honed on the job. Providers interviewed felt that they had sufficient subject matter expertise to effectively disseminate FITA information.

PREPARATION FOR BRIEFINGS

Headquarters makes materials available to the field installations, but there is no requirement that the materials be used. As indicated above, each field installation has considerable autonomy. Source materials for briefings are obtained from CIA, DIS, DoDSI, DOE, FBI, NACIC, NSA, and PERSEREC. Additional materials and information are developed by individuals located in the field installations. A notable example is *Threat Summary*, published periodically by the Johnson Space Center.

RECOMMENDATIONS

Persons interviewed at NASA offered a number of suggestions for improvements. The resources available to the security program should be increased. These resources could be used to support additional training for security personnel and to develop improved materials for use in communicating security-related information to NASA personnel.

A centralized database that contains a template of interests of various government (DoD and non-DoD) agencies should be developed. This would facilitate sharing of information and materials and would improve interagency communication and cooperation. Access to the INTELINK should be easier.

A mechanism should be established for resolving different threat evaluations arising from different sources (a "one-stop" shopping approach). NACIC could play a central role in accomplishing this goal.

Criteria should be developed for evaluating the effectiveness of security programs. This effort should draw on the expertise and experience of representatives from various government agencies. Possible criteria could include the number of reports filed for investigation (relative to population size and agency mission) and various actions resulting from the reports (e.g., the number of clearances denied).

Appendix F-18

AGENCY	NATIONAL COUNTERINTELLIGENCE CENTER (NACIC)
HQ POINT OF CONTACT	Catherine M. Kiser Community Training Branch

BACKGROUND

NACIC was established in August 1994 to coordinate national counterintelligence policy and activities. These activities include facilitating the development and implementation of interagency counterintelligence training programs, developing all-source assessments of the foreign intelligence and other related threats to U.S. national and economic security, interfacing with national security countermeasures programs, integrating counterintelligence community databases, providing effective secretariat support to entities of the national counterintelligence structure, and assessing the overall effectiveness of the national counterintelligence program.

NACIC is comprised of three subordinate offices: the Program Integration Office, the Threat Assessment Office, and the Executive Secretariat Office. It is the activities of the Program Integration Office that most directly relate to FITA. This office is responsible for a number of initiatives to disseminate threat information to the private sector.

NACIC operates under the authority of the National Counterintelligence Policy Board, in accordance with Presidential Decision Directive/NSC-24, *U.S. Counterintelligence Effectiveness*, May 3, 1994, and consistent with the recommendations in Presidential Review Decision/NSC-44, Apr 30, 1994). PDD/NSC-24 called for improved U.S. counterintelligence effectiveness by enhancing integration and cooperation among various U.S. counterintelligence agencies.

SCOPE

With the creation of the NACIC, counterintelligence information reaches the security countermeasures community, other U.S. government agencies, and the U.S. private sector in a coordinated, more frequent and timely basis. The NACIC's Community Training Branch, in cooperation with a variety of industry associations, sponsors regional awareness seminars for private-sector security officers and other relevant private-sector managers. The purpose of these seminars is to present industrial security decisionmakers with "integrated" community counterintelligence information and, equally important, to point out the local resources available to their companies' counterintelligence awareness programs. Since 1995, the NACIC has sponsored 12 regional seminars in locations throughout the U.S. Through these seminars, the NACIC

strives to bring together a variety of different speakers from the counterintelligence community who can provide up-to-date threat data on issues of concern to the private sector. The response to these seminars has been very significant and the NACIC is overwhelmed with requests from U.S. industry to provide unclassified threat data that can be disseminated to employees in an effort to educate them on significant security issues.

The National Counterintelligence Policy Board approved seven recommendations by the NACIC for improving counterintelligence support of the private sector. One recommendation directs the NACIC to establish a working group to evaluate and coordinate the counterintelligence community's industrial briefing and awareness programs. In October 1994, the first meeting was held for those government agencies having awareness programs that focus on the private sector. This interaction among representatives of different government agencies was the beginning of the NACIC's Awareness Working Group (AWG). At this time 21 U.S. government agencies are represented.

The formation of this AWG has succeeded in substantially reducing the duplication of effort that existed in the past. The strategy of the AWG is to have the counterintelligence community consider the U.S. private sector as a significant consumer of, and contributor to, government intelligence. Jointly, the AWG will create analytical products for the private sector on specific collection techniques and the methods of operations of foreign entities that target industry's proprietary data, U.S. government contracts, employees, or facilities. In addition, the AWG will identify and promote "excellence in threat awareness programs, publications, and speakers."

Members of the AWG have shared awareness materials and developed new products, such as a security awareness video produced by the FBI, DOE, and the NACIC entitled, *Something Wasn't Right.* In addition, the NACIC has published a document identified as *Counterintelligence Awareness Programs* which was created by the members of the AWG to highlight the various counterintelligence awareness programs that are available from U.S. government agencies. This publication is unclassified and has been distributed at all regional seminars. The AWG meets on a regular basis to discuss issues of concern to the counterintelligence community and has, to this date, achieved success in resolving issues of concern.

NACIC personnel are routinely called upon to participate in seminars and other security forums to address current issues such as economic espionage and other related areas of interest to U.S. government and private sector audiences.

Appendix F-19

AGENCY	NATIONAL IMAGERY AND MAPPING AGENCY (NIMA)
HQ POINT OF CONTACT	Leslie E. Howell Mission Security Support Officer

BACKGROUND

The National Imagery and Mapping Agency is the newest member of the intelligence community. Its mission is to provide timely, relevant, and accurate imagery, imagery intelligence, and geospatial information in support of national security objectives. NIMA was established in October 1996, combining different parts of the Defense Mapping Agency, Central Imagery Office, National Reconnaissance Office, and Defense Intelligence Agency. Having its origins in both civilian and defense organizations, NIMA has a unique place within the intelligence community and a unique relationship to the DoD.

NIMA is organized into three distinct business units: Operations, Systems and Technology, and Corporate Affairs. Within Corporate Affairs is Mission Support (MS) with East and West Regional Commanders who oversee multiple locations, each with its own Site Security Officer. Also within MS is the Mission Support Service (MSS) whose Mission Support Security Service Division (MSST), Office of Counterintelligence and Security Awareness, is responsible for counterintelligence awareness. Within this Office resides the CI Awareness Team (CATeam) which is responsible for all counterintelligence-related training.

NIMA derives counterintelligence-related policy guidance from E.O. 12333 *U.S. Intelligence Activities* (Dec 4, 1981); E.O. 12968 *Access to Classified Information* (Aug 4, 1995); PDD/NSC-12 *Security Awareness and Reporting of Foreign Contacts* (Aug 5, 1993); DCID 1/14 *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information* (Jan 22, 1992), DoD 5200.1R *Information Security Program*, DoD S-5105.21-M-1 *Sensitive Compartmented Information Administrative Security Manual, Communication Intelligence Policy,* and DoD TS-5105.21-M-3 *Sensitive Compartmented Information Administrative Security Manual, TK Policy.* NIMA is currently in the process of translating these policies into various implementation policy directives and regulations.

SCOPE

The CATeam consists of three members--a leader and two team members. This team has the sole responsibility for developing and presenting counterintelligence-related briefings to all NIMA civilian employees as well as military assignees and contractors/consultants. Briefings include the following: counterintelligence awareness; security awareness; OPSEC; Counter-Terror; travel; intelligence; annual refresher SF312 (covering storage, discussion, and handling of classified information); anomalies; and specialized briefings, such as tour guides, marking requirements, threat to special programs, etc.).

The NIMA CATeam has expended considerable in-house time and resources to develop and implement its counterintelligence awareness program, including counterintelligence awareness, security awareness and travel briefings. The CATeam presents group counterintelligence awareness and security awareness briefings on an annual basis at all NIMA locations, group travel briefings monthly, and individual counterintelligence awareness and travel briefings on an individual basis, as needed.

These NIMA briefings are given by the CATeam, using a unique team-training approach in conjunction with professional multi-media presentation materials. In the future, these briefings will be videotaped so that they can be used to brief hard-to-reach audiences (e.g., those working on night shifts, in remote locations, or who miss the group presentations). This well-developed program demonstrates NIMA's management and counterintelligence staff's commitment to a proactive FITA program with direct relevance to the organization.

PROVIDERS' BACKGROUND AND TRAINING

The three NIMA CATeam providers were selected because of their extensive experience in the security area and in counterintelligence. The team leader's counterintelligence-related experience in the military and other government agencies is complemented by other team members' experience in physical, computer, information and personnel security. The CATeam members believe that their diverse backgrounds have allowed for the development of more effective and interesting presentations.

Training received by the CATeam to make effective presentations includes courses given by DIA (SCI Security Officer's Course), DoDSI (e.g., Concepts in Security Awareness, Security Specialist Course, Information Security Course, Brief the Briefers), NSA (e.g., Operations Security Course), and SAES (e.g., Espionage Then and Now, Security Educator's Course). Also, CATeam members have attended college courses on conventional security threat and protection and in-house courses on the use of media (e.g., PowerPoint©). Most of their training has been on-the-job, although the providers have been pleased with the formal training they have received and would welcome the opportunity for additional relevant training, especially counterintelligence courses.

PREPARATION FOR BRIEFINGS

The providers believe that they are very well prepared to design, develop, and present FITA presentations. They spend considerable time collecting and regularly updating information so that it is current, interesting, and relevant to NIMA. This information is gathered from newspaper articles, databases on the Internet, security publications, and personal and on-the-job experiences. Organizations listed as the most helpful in providing source materials for creating briefings include CIA, DIA, DoDSI, NACIC, and NRO. Also listed were the American Society for Industrial Security (ASIS), the National Classification Management Society (NCMS), and the Security Awareness Education Subcommittee (SAES).

While the counterintelligence awareness and security awareness briefings are generic and designed for all NIMA audiences, the briefings are tailored to some extent for targeted audiences, specifically for travelers (Travel Brief), tour guides (Tour Guide Brief), and administration (Administrative Brief). Examples of such targeting are the Supervisors Security Training (a security training program designed for supervisory personnel), Security Monitors Training (a program developed to train agency personnel to provide in-house assistance to the security offices), and the NIMA Traveler's Package (a package of travel information prepared and tailored to the specific country to which the employee is traveling. This folder is updated regularly and is available to all NIMA employees and contractors upon request whenever they plan business or personal travel to a destination outside the United States).

RECOMMENDATIONS

Persons interviewed at NIMA offered a number of suggestions for improvements in the FITA program:

On the policy level, there should be a standard threat awareness policy for all agencies. In order to be effective, this policy needs to be given priority on a national level and needs to be supported by agency upper-level management. Only with such support can an agency's counterintelligence program have the opportunity to be effective.

On the practical level, there was interest in the development of a common counterintelligence database and repository of materials accessible to all agencies. This centrally developed and maintained database and repository should include such relevant information as the status of current regulations and changes to these regulations, current threat information, available briefings and contacts for obtaining the briefing materials and handouts, training sources and materials, news updates on issues and on what's happening in the security area, and announcements on up-coming events and courses related to counterintelligence awareness.

Appendix F-20

AGENCY	NATIONAL RECONNAISSANCE OFFICE (NRO)
HQ POINT OF CONTACT	COL Phillip B. Pounds Director of Counterintelligence

BACKGROUND

NRO is a hybrid organization, set up by a Memorandum of Understanding between the Deputy Secretary of Defense and the Director of Central Intelligence (DCI). Its government personnel are drawn largely from CIA, Air Force, and Navy. Counting contractors, NRO has over 60,000 employees, with a 20:1 ratio of contractors to government employees.

The highest priorities in NRO's counterintelligence awareness program are to convince government and contractor personnel that the threat really is serious and to enhance ability to recognize indicators of possible hostile interest or activity. Some of the same technology used in highly classified reconnaissance systems is now being used in commercial systems being developed in joint ventures with foreign countries. The guidelines on what needs to be protected are not always clear. Formerly classified contractors are entering the open, while also being told that the foreigners they are now dealing with are trying to steal their secrets.

In addition to the applicable executive orders, DCI directives and DoD regulations, NRO is guided for counterintelligence policy by internal memoranda and directives that outline reporting requirements for foreign contacts and travel and set the standards for awareness briefings for affected employees.

SCOPE

NRO's principal briefings are its 50- to 90-minute General Audience Counterintelligence Awareness/Threat Overview, and its 20- to 30-minute Executive Level Current Threat Briefing. As needed, it also puts on a longer training session for counterintelligence and security professionals.

The counterintelligence office has four people who give presentations, including the director. One works full time on training and awareness presentations, one 30% to 50%, and one 30%. Potential plans call for adding four more people to the staff this year. Additional briefings are also given by security officers of the various contractors.

Most of the awareness briefings are given to an audience of 200 to 250. NRO makes a distinction between awareness briefings and awareness training. Most of the

contractor briefings last less than one hour, because these are billable hours for the contractor personnel. Training is a longer session focused on a subset of people who need the training to perform their specific tasks, e.g., security personnel are trained to give briefings to employees of their organization.

NRO Security has a Training and Education Division that prepares security education materials including a periodic newsletter, brochures, videos, and posters. An Instructional Technology Branch prepares computer assisted training.

PROVIDERS' BACKGROUND AND TRAINING

Providers have extensive experience in counterintelligence or security at the GS-13 to GS-15/0-6 level. They are trained and experienced in presentation techniques before coming to the job.

PREPARATION FOR BRIEFINGS

NRO sees a dramatic improvement during the past 3 to 5 years in various agencies' willingness to make threat-relevant information available in a form that can be used by contractors. There is a lot more willingness to share information, and INTELINK makes it easier to share. The office now has more information than it can use in the time available for briefings.

NRO field sites and contractors also provide a steady flow of counterintelligence reports, so briefings now draw heavily on NRO's own experiences. To stay current, NRO tries to avoid citing cases or incidents that occurred prior to 1992, but this is sometimes difficult. Everyone wants a smoking gun, but it is often not there, can't be talked about, or is so old you don't want to mention it.

RECOMMENDATIONS

NRO has found that audiences appreciate a little bit of humor, and that they want to hear war stories about actual experiences. If one can talk from personal experience, it adds credibility.

Top management support of the program is not a problem. The major challenge is the very large number of people to be educated. It is the same problem that any priest or rabbi has: the people who come to hear you are not necessarily the ones you most need to reach.

Appendix F-21

AGENCY	NATIONAL SECURITY AGENCY (NSA)
HQ POINT OF CONTACT	Donna Pucciarella, Chief Counterintelligence/Security Awareness Counterintelligence Services Office of Security Services

BACKGROUND

NSA is the nation's cryptologic organization, tasked with making and breaking codes and ciphers. The agency is charged with two of the most important and sensitive activities in the U.S. intelligence community. The information systems security (INFOSEC) mission provides products and services to protect classified and unclassified national security systems against exploitation; and the foreign signals intelligence (SIGINT) mission consists of all the foreign signals collection and processing activities in the U.S.

NSA is divided into five directorates. Counterintelligence/Security Awareness falls under the Deputy Director of Security for Counterintelligence in the Directorate of Support and provides counterintelligence/security awareness services to the other five directorates.

NSA derives counterintelligence-related policy guidance from E.O. 12333 *U.S. Intelligence Activities* (Dec 4, 1981); PDD/NSC-12 *Security Awareness and Reporting for Foreign Contacts* (Aug 5, 1993); E.O. 12968 *Access to Classified Information* (Aug 4, 1995); DCID 1/14 *Personnel Security Standards and Procedures Governing Eligibility for Access to SCI* (Jan 22, 1992); and DoD Directive 5240.6 *Counterintelligence Awareness and Briefing Program* (Jul 16, 1996). These larger policies are translated by NSA into literally dozens of policy issuances and regulations regarding separate facets of the NSA counterintelligence program.

SCOPE

Counterintelligence/Security Awareness, with a staff of five presenters, briefs all NSA employees and affiliates, including civilians, military assignees, and contractors/consultants. Briefings include indoctrination; orientation (which includes discussion of the threat); foreign travel briefings (as a group, one-on-one, or by video); courier briefings; reawareness briefings; debriefings; and special access briefings. Foreign intelligence threat and defensive counterintelligence countermeasures are included in all awareness briefings, thus ensuring awareness programs that are directly threat-based.

The different kinds of stage briefings at NSA Headquarters are scheduled for fixed days of the week while special travel briefs are scheduled on an as-needed basis.

All briefing attendees are surveyed after each briefing and, in some cases, are followed up with their supervisors to see if the briefing was effective, i.e., that how-to behavior was learned and followed successfully.

NSA also has a popular series of Continuing Awareness presentations held in the large auditorium at Headquarters and internally broadcast on the NSA network. These presentations are also videotaped and made available for use by NSA and DoD affiliates. Quarterly infomercials are produced--short video updates on CI/Security--which are shown on the NSA broadcast network between programming. There is also an extensive publications division under CI/Security Awareness which produces brochures, posters and other materials, for NSA employees and for the counterintelligence community.

NSA leverages its briefings to industry by training Contractor Special Security Officers (CSSOs) who after two courses at NSA will return to their companies as NSA-sponsored providers. To augment these NSA-trained contractor providers, HQ staff travel from time to time throughout the country on a traveling roadshow, delivering special briefings to their contractors in situ. And NSA presenters sometimes brief at conferences and other counterintelligence community gatherings. NSA also offers counterintelligence training to SIGINT analysts and reporters four times a year, and trains supervisors and managers in regular courses.

PROVIDERS' BACKGROUND AND TRAINING

All providers are NSA special agents. All have served as investigators, and most as adjudicators in personnel security or inspectors in facilities security (HQ/field/industrial). Some have worked in other parts of the counterintelligence organization at NSA. They have all had relevant security training when they arrive, but receive briefings skills and on-the-job training when they join the department. Some training courses are internal to NSA; others are held at the FBI Academy or at the CIA. And the providers also are encouraged to hone their skills and knowledge as they mature in their jobs.

PREPARATION FOR BRIEFINGS

Providers at NSA advise that their presentations are fairly well scripted. A standard syllabus has developed over time to which each presenter makes his/her own adaptations. In addition, each provider is an expert on one particular part of the world (e.g., China; SE Asia; Russia, etc.) and spends much time searching on-line for information--to update travel briefings, for example. Each provider researches material for espionage case studies for use during briefings.

Sources of information for the providers differed slightly from person to person (as did judgment of quality and availability), but they draw their information from: CIA, DIA intelligence reports, DIS, DoDSI, DOE, FBI, FAA Safety Bulletins, INTELINK, NACIC, and NRO, plus NSA's own internal computerized databases. Some materials come to them automatically. But often the providers have to call for information, frequently using their personal friends/contacts in these organizations. This takes time, and they would prefer to get the information automatically.

RECOMMENDATIONS

Persons interviewed at NSA offered a number of suggestions for improvements:

The principal government security awareness committee, the Security Awareness and Education Subcommittee (SAES) of the Security Policy Board, requires funding to be effective. They must rely on the donated time and resources of participating agencies and, in the current fiscal climate, education efforts are suffering.

While most intelligence community agencies provide adequate initial indoctrination and orientation programs for new employees, they should concentrate additional resources to address continuing counterintelligence/security awareness and education programs for on-board affiliates. Particular attention should be given to system administrators and managers.

Knowledge of information system security vulnerabilities, exploitation of computers by foreign intelligence services, and similar issues is woefully lacking in the counterintelligence community. Consequently, standard security briefings are weak in this area. The NACIC or SAES should concentrate efforts and funds to develop briefing modules for use by government and industry on this topic.

The providers we interviewed at NSA felt that more resources should be made available for FITA, especially so that the NSA roadshow program can be expanded. While they were basically satisfied with their training, they would naturally enjoy more, if resources were available.

While the providers have access to numerous computerized sources of counterintelligence information, they emphasize the importance of personal contact with their counterparts in other counterintelligence agencies. It's often by calling these "links" in other agencies that they get their best information and in the most timely manner. They recommend opening interagency channels on a more formal basis so that information can be routinely and conveniently exchanged among the various agencies presenting threat awareness programs.

One provider urged that the counterintelligence world should never go to purely computer-based security education, without a human being involved to interpret. Real-live people should also introduce, interpret and explain any counterintelligence videos.

Appendix F-22

AGENCY	NAVAL CRIMINAL INVESTIGATIVE SERVICE (NCIS)
HQ POINT OF CONTACT	John Daniels III Special Agent Training Directorate

BACKGROUND

NCIS is the agency within the Department of the Navy (DON) with the primary responsibility for criminal investigation and counterintelligence. Support to all Navy and Marine Corps commands in executing their responsibility for maintaining good order and discipline is the mission of NCIS. The NCIS counterintelligence mission is to provide timely, relevant, and anticipatory counterintelligence support throughout the full range of military operations to all levels of command within the Department of the Navy.

NCIS derives counterintelligence-related policy guidance from E.O. 12333 *U.S. Intelligence Activities* (Dec 4, 1981); E.O. 12968 *Access to Classified Information* (Aug 4, 1995); PDD/NSC-12 *Security Awareness and Reporting of Foreign Contacts* (Aug 5, 1993); DCID 1/14 *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information* (Jan 22, 1992); DoD 5240.1-R *Procedures Governing the Activities of DoD Intelligence Components That Affect U.S. Persons* (Dec 82); DoD-2000.12 *DoD Combating Terrorism Program* (Sep 13, 1996); DoD-2000.14 *DoD Combating Terrorism Program Procedures* (Jun 15, 1994); and DoD-5240.6 *Counterintelligence Awareness and Briefing Program* (Jul 16, 1996). These policies are translated into various implementation policy directives and regulations, including SECNAVINST 3875.1 *Counterintelligence and Awareness Briefing Program* (Nov 2, 1988) and OPNAVINST 5510.1H *Department of the Navy Information and Personnel Security Program Regulation* (Apr 29, 1988).

SCOPE

NCIS Headquarters is located in Washington, DC. There are about 150 NCIS offices located around the world, including 14 major field offices. Counterintelligence briefings are presented by about 280 Foreign Counterintelligence (FCI) agents to all Navy and Marine Corps military personnel and DON civilians, including both inhouse and selected contractor personnel.

PROVIDERS' BACKGROUND AND TRAINING

All NCIS agents are at least 21 years of age, have completed 4 years of college, and have passed two background investigations (DIS and NCIS). The minimum clearance level is Top Secret, and most agents are cleared for higher levels. Agents assigned to FCI billets with briefing responsibilities receive their training from experienced agents in the office and through experience on the job.

PREPARATION FOR BRIEFINGS

Initially, the provider introduces the general topic of counterintelligence, tailoring the information to the audience. The major portion of a FITA briefing consists of a videotape, *Espionage: A Continuing Threat.* Once the videotape is over, the agent completes the briefing by providing information about reporting procedures and answering any questions from the audience. Finally, the agent stays around for a period after the briefing to discuss any issues which audience members wish to discuss in private.

This videotape is quite good. Narrated by John Walsh (from the television show, *Most Wanted*), it covers a wide range of counterintelligence topics in about 20 minutes. Use of this videotape ensures that a consistent message is delivered to all the audiences. Unfortunately, at this point, the tape is somewhat dated. Many people in briefing audiences have already seen it.

In preparing for presentations, agents obtain most of their information and materials from within NCIS. Other sources mentioned included ANSIR, CIA, DIS, DoDSI, NACIC, and NSA. The vast majority of persons interviewed felt that they had sufficient subject matter expertise to effectively communicate foreign intelligence threat awareness information. In addition, in evaluating their presentation skills, they felt well prepared to find the resources needed to develop and deliver counterintelligence information, design and develop materials, speak before audiences, and hold their attention.

RECOMMENDATIONS

Persons interviewed in NCIS offered a number of suggestions for improvements. Counterintelligence awareness should become a priority for the Navy. Commands frequently view counterintelligence briefings as time-consuming and an interference with operational duties. Briefings are sometimes postponed until just before an IG review. (Security awareness is one item of interest in the inspection).

A consistent policy should be promulgated by DoD for counterintelligence awareness briefings. This policy should specify attendance requirements, and should include all employees, not just those with security clearances.

Funding should be dedicated to producing and maintaining an up-to-date, high quality, standardized awareness briefing designed for DON personnel. This briefing would replace the somewhat outdated videotape.

Appendix F-23

AGENCY	NUCLEAR REGULATORY COMMISSION (NRC)
HQ POINT OF CONTACT	Wayne Burnside Information Security Specialist

BACKGROUND

The NRC is a relatively small agency whose primary mission is to ensure adequate protection of the public health and safety, the common defense and security, and the environment in the commercial use of nuclear materials in the United States. The agency's scope of responsibility includes regulation of commercial nuclear power reactors; nuclear power research, test, and training reactors; fuel cycle facilities; medical, academic, and industrial uses of nuclear materials; and the transport, storage, and disposal of nuclear materials and waste. NRC's mission is carried out by a relatively stable population of 3,000 employees, 2,000 of whom are located at its headquarters in Rockville, Maryland. All NRC employees are cleared at the Top Secret (Q) or Secret (L) level. Among these employees are highly technical nuclear engineers.

Within the NRC, the Division of Facilities and Security is located in the Office of Administration under the Deputy Executive Director for Management. The Division of Security plans, develops, establishes, and administers policies, standards, regulations, and procedures for the overall NRC security program. It includes information security, personnel security, and physical security personnel at NRC headquarter's facilities and regional offices and at contractor, licensee, certificate holder, and other facilities. Within the Division of Facilities and Security, the Information Security Branch is responsible for foreign threat awareness education and training.

The NRC derives counterintelligence-related policy guidance from various directives, including E.O. 12333 *U.S. Intelligence Activities* (Dec. 4, 1981); E.O. 12968 *Access to Classified Information* (Aug 4, 1995); PDD/NSC-12 *Security Awareness and Reporting of Foreign Contacts* (Aug 5, 1993); and DCID 1/14 *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information* (Jan 22, 1992).

SCOPE

Being a very small agency with limited human and financial resources, the NRC does not have a FITA program per se. Instead, it relies upon a single provider within the Information Security Branch to develop and disseminate threat awareness information as an integral part of its overall security program. This provider disseminates general

counterintelligence awareness information during newcomers briefings and general and special counterintelligence information to foreign travelers to designated countries and to supervisors of the Foreign Assignee Program.

At the newcomers briefings, general threat awareness information may be communicated via the video, *Something Wasn't Right*, which was developed by the Department of Energy, the FBI, and NACIC. Specific threat awareness information is presented to NRC employees via written foreign travel briefings and memos. While few NRC employees travel abroad, those who do are often highly technical nuclear engineers. International travel briefs are disseminated via interagency memos with attachments to employees with travel orders to particular countries of special concern; travelers to other countries also receive travel information upon request. These attachments contain information tailored to the specific country of destination including the techniques used and information sought by foreign collectors. In an average year, approximately 75 written travel briefs are distributed, and structured debriefs are conducted with a percentage of those returning from foreign travel to the special countries of concern.

NRC is also concerned about the vulnerability of those who work within the Foreign Assignee Program in which other governments exchange technical personnel with the United States. These exchange personnel, who are often from third world and developing countries, work with NRC engineers to learn how the United States regulates nuclear power. As part of NRC's awareness program, the provider develops written counterintelligence awareness briefs which are presented to the supervisors before the assignees arrive and again at the mid-point of their visit. Also, the assignees are interviewed mid-way through the program; they are not, however, debriefed before returning to their country of origin.

PROVIDERS' BACKGROUND AND TRAINING

At NRC, the individual responsible for disseminating foreign threat awareness information is selected from among those with backgrounds in information security. This individual does not receive formal training in giving effective briefings; instead, experience is gained on the job. The current provider indicated that training on topics related to counterintelligence, perhaps given by NACIC, would be helpful.

PREPARATION FOR BRIEFINGS

The NRC provider reported being well prepared to design, develop, and present counterintelligence presentations. For the most part, the provider creates his own briefings, tailoring them to specfic NRC audiences. A small portion of the briefing materials are adapted from newspaper articles, security seminars, and security publications. Materials also are gathered from other agencies in the counterintelligence community including the Department of Energy, FBI, NACIC, and the State Department.

Most valuable in the development of NRC's travel briefings is information acquired from the Pinkerton Risk Assessment Service and from information provided by the State Department, such as Consular Information Sheets and Travel Warnings.

RECOMMENDATIONS

The NRC provider offered a number of suggestions for improvements in the counterintelligence program:

Specific information on the changing threat from military to economic would be particularly useful. This information should include how the threat is changing, what information is being sought and by whom, and the extent to which other countries are seeking U.S.'s nuclear technology.

There needs to be an improved method for exchanging counterintelligence-related ideas and information among the various agencies. Also, better ways are needed to communicate with employees. An intelligence community intranet may serve this function well.

Additional products for use in briefings would be helpful, especially to agencies with smaller counterintelligence programs and operating with limited counterintelligence financial and human resources.

Appendix F-24

AGENCY	OFFICE OF THE SECRETARY OF DEFENSE (OSD)
HQ POINT OF CONTACT	John J. Ziegler III Assistant Deputy Director of Counterintelligence Office of the Deputy Assistant Secretary of Defense (ODASD) Intelligence & Security (I&S)

BACKGROUND

Oversight coordination for counterintelligence in OSD comes directly from the National Security Council, down through the National Counterintelligence Policy Board (NACIPB) and the National Counterintelligence Operations Board (NACOB), with input from the Director of Central Intelligence (DCI) and from the National Counterintelligence Center (NACIC).

Funding of DoD's counterintelligence program is managed by the Director of Counterintelligence, OSD. Funds come from the National Foreign Intelligence Program (NFIP), through the Foreign Counterintelligence Program (FCIP), to the military services, DIA, DIS, NSA and OSIA. Other sources of counterintelligence funding include Security and Investigative Activities, and Tactical Intelligence and Related Activities (TIARA). OSD's Director of Counterintelligence works closely with CIA, FBI, NACIC and other national-level counterintelligence organizations, and coordinates the writing of directives and policy.

OSD staff conduct several oversight visits per year to the various counterintelligence components. They do not have a formal evaluation program of FITA efforts. They do, however, conduct other counterintelligence program reviews with the Services, especially in the areas of investigations and operations. They also ask the Services to provide updates on any significant developments, such as late-breaking espionage cases, so that they, in turn, can report to the Secretary of Defense.

The major counterintelligence-related policies and directives written by OSD (or affecting OSD) include DoD Directive 5240.1 *Activities of DoD Intelligence Components that Affect U.S. Persons* (Dec 3, 1982); DoD Directive 5240.1R *Procedures Governing the Activities of DoD Intelligence that Affect U.S. Persons* (Dec 1982); DoD Directive 5240.2 *DoD Counterintelligence* (Jun 6, 1983) (an updated version is to be released shortly); DoD Directive 5240.6 *Counterintelligence Awareness and Briefing Program* (Jul 16, 1996); and PDD/NSC-12 *Security Awareness and Reporting Foreign Contacts* (Aug 5, 1993).

SCOPE

This Office itself does not conduct counterintelligence briefings. Counterintelligence support to the Office itself is rendered by AFOSI.

Appendix F-25

AGENCY	ON SITE INSPECTION AGENCY (OSIA)
HQ POINTS OF CONTACT	LCOL James E. Wright Deputy Chief, Office of Counterintelligence CW5 J. W. Harper Chief, Counterintelligence Operations

BACKGROUND

OSIA was created 10 years ago as an executing arm of the DoD to implement on-site inspections mandated by the Intermediate Nuclear Forces Treaty (INF). Since that time the agency has been involved in the implementation of many additional treaties and treaty-like agreements. These include the Threshold Test Ban Treaty, the Chemical Weapons Agreements, the two Stratetgic Arms Reduction Treaties, Conventional Armed Forces in Europe Treaty, the Vienna Documents, the UN Special Commission on Iraq Support, Operation Provide Hope in FSU, Defense Treaty Inspection Readiness Program, Open Skies Treaty, and the Dayton Accord.

The agency's mission includes sending teams to inspect for and verify treaty provisions in the former Soviet Union and other countries. In turn, it supports inspections of U.S. military and government facilities by the Russians and others in this country, providing escorts, translation, transportation, care and feeding, etc. for these guests. About two-thirds of OSIA employees rotate in from the military, mostly from the Air Force and Army.

Government policies covering OSIA include the classified NSD-296 and various other classified PDDs and Directives regarding the different treaties. OSIA directive, OSIA 5240.2 *Conduct of OSIA Personnel* (Mar 5, 1996), details rules of behavior for personnel on OSIA missions. OSIA is also guided by the other major DoD Directives, such as *DoD 5240.2, DoD Counterintelligence* (Jun 6, 1983), DoD 5240.6, *Counterintelligence Awareness and Briefing Program* (Jul 16, 1996), and DoD Directive 2000.12 *DoD Combatting Terrorism Program* (Sep 13, 1996), etc.

SCOPE

A U.S. inspection team going abroad typically consists of 10 individuals: a team chief and deputy team chief (with expertise in the appropriate treaty provisions), two linguists, and about six other individuals with technical weapons expertise.

All OSIA personnel assigned to duty in the former Soviet Union and other specified states must receive a safety/security briefing prior to, and subsequent to, the mission. Similar briefings are mandatory for OSIA personnel on escort duty in the U.S. Briefings take place at the Dulles Airport office and three other locations around the world. They are given (at Dulles) by a team of five providers on an as-needed basis. In FY95 some 264 teams were briefed. Audiences are small and the message focused on the specific mission.

PROVIDERS' BACKGROUND AND TRAINING

All OSIA providers have been trained in special agents counterintelligence courses in their military service so they share a common body of knowledge with colleagues at OSIA. The special agents come from Army Counterintelligence, Air Force Office of Special Investigations, and the Naval Criminal Investigative Service.

PREPARATION FOR BRIEFINGS

The providers we talked with at OSIA prepare their FITA material by consulting both classified and unclassified sources. Intelligence community databases such as INTELINK, open-source materials on the Internet, and general newspaper/magazine articles are their main sources of information. They also acquire information from DoDSI and NACIC and from several nongovernment organizations. A great deal of their information comes from others at OSIA itself. For example, the agency has its own counterintelligence analysis section. The briefings are tailored specifically for the target audience and address issues concerning current missions.

RECOMMENDATIONS

One provider suggested that a formal conference be convened among the different counterintelligence components of the counterintelligence community to get up to speed on what other agencies are doing, with a view to sharing information.

Another would like a wider base of reference material and would like to see current espionage cases declassified as soon as possible to illustrate the latest foreign intelligence service methods, targets, etc.

Appendix F-26

AGENCY	SECURITY POLICY BOARD (SPB or Board)
HQ POINT OF CONTACT	James D. Passarelli Staff Member

BACKGROUND

In 1993, 10 prominent Americans assembled to address significant security issues of the 1990s and beyond. This group, known as the Joint Security Commission (JSC), was charged with formulating recommendations that would cause government agencies with national security concerns to effectively balance costs with adequate security. The JSC concluded that the only way to end policy fragmentation and ensure security reciprocity and security cost-effectiveness throughout the government was to establish and empower an organization akin to the SPB. The Administration established the Board in September 1994 with Presidential Decision Directive-29 (PDD-29). The PDD-29 charged the Board with establishing a new policy development process that would result in more cost-effective security without diminishing the effectiveness of the U.S. security apparatus. An annual report is provided to the President through the Assistant to the President for National Security Affairs in order to afford the Administration an opportunity to measure progress in this regard.

The Board, with its substructure of the Security Policy Forum (Forum), five standing committees, and ad hoc working groups, all regularly kept informed by key industrial representatives, has served to facilitate reciprocity and commonality by engaging 34 federal agencies and departments in the dialogue and process that lead to national policy formulation. The Board, composed of 10 deputy secretaries or under secretaries or equivalent, functions primarily to rule on policies formulated by the Forum and standing committees and, when required, resolve conflicts that arise in the substructures. The process of policy development now moves at a much quicker speed and enjoys governmentwide buy-in by member agencies and departments.

The Board has made significant strides in eliminating the fragmentation that exists in the security policy structure in the U.S. It has served to provide leadership, focus, and direction to the government's security community. Through its structure the Board is developing unified policy that is based on sound risk management; is in consonance with the oberall goals of PDD-29; takes into account the diverse threats our nationa now faces; and recognizes a renewed interest and respect for the public's right to know.

One committee of particular interest in relation to FITA is the Board's Threat Requirements Committee. This interagency committee, established under the Policy Integration Committee in September 1996, addresses issues concerning the dissemination of accurate and timely threat data. The committee assembled a comprehensive intelligence production requirements statement. The document identifies intelligence information that various members of the security countermeasures community need in order to successfully perform their protective missions. The intent is to provide appropriate producers of intelligence with a comprehensive requirements list from which members of the security countermeasures community can select items relevant to performing their specific protective functions. The Board sees this as a first step in developing an effective, efficient process in supporting dissemination of threat information to the countermeasures community. This effort should produce a process to ensure that threat information is disseminated in a timely manner to the appropriate countermeasures community requesters and that dissemination extends, as appropriate, to their counterparts in industry.

SCOPE

The Board does not conduct counterintelligence briefings. Counterintelligence support to the Board is rendered by a variety of SPB member department and agency counterintelligence components on an as-needed basis.

Appendix F-27

AGENCY	SENATE
HQ POINT OF CONTACT	Michael P. DiSilvestro Director of Security

BACKGROUND

The Senate is by design an open organization. However, certain individuals in the Senate, because of their roles and access to information, present attractive targets for the many foreign intelligence officers who, along with the public, freely roam the halls. Large quantities of highly classified information make their way to the Senate from the Executive Branch and are stored in small islands of security. While the traditional target has been the trio of military, political and intelligence information, recently foreign intelligence services have begun looking for nonclassified, technical information, of which much abounds in the various committees of the Senate. From senator to aide to clerk, all who work at the Senate are potential targets.

SCOPE

The Office of Security was established in 1987. Until then, the system of protecting classified information and issuing security clearances was handled by the Executive Branch, and security and counterintelligence briefings were conducted on an ad hoc basis.

The Senate Office of Security consists of five people, two of whom conduct security and FITA briefings. Each of the 100 senators and every separate committee has a security manager, in all numbering 130. Some 3,000 people work in the Senate building; of these only 500 are cleared. SCI access is given only to committee and leadership staff whose duties require it.

Every Senate employee is given an initial security briefing. After the clearance is granted, a yearly refresher briefing is required. An effort is made to give people concrete examples of real cases and incidents in order to emphasize the special vulnerability of the Senate environment. While the Office of Security conducts regular security and awareness briefings, the AFOSI, CIA, FBI, NSA, and State are often invited to give special briefings.

Senators are entitled to broad information access by virtue of their constitutional office; background investigations and clearances are, therefore, not required. Senators are given a series of special orientation briefings when they first come to the Senate.

The Senate has its own internal organizational intranet, and a homepage, presently under development, will host ongoing security education and awareness campaigns. Security doesn't produce any posters or pamphlets themselves; they borrow from the Eecutive Banch, notably CIA, DIA and NSA. It does, however, produce a quarterly newsletter which often is a compilation of recent counterintelligence and related articles, or articles answering frequently asked questions.

PROVIDERS' BACKGROUND AND TRAINING

The Director of Security has a master's degree in security policy studies and has received additional security training at NSA, FBI and DIA. His deputy was formerly in the Army, working at INSCOM, OSD, NASA and DOE.

PREPARATION FOR BRIEFINGS

No information

RECOMMENDATIONS

No information

Appendix F-28

AGENCY	DEPARTMENT OF STATE (DS)
HQ POINT OF CONTACT	Nanette Krieger, Chief Counterintelligence Division

BACKGROUND

The Department of State is the lead U.S. foreign affairs agency. It advances U.S. objectives and interests by formulating, representing, and implementing the President's foreign policies. The department carries out its mission through overseas posts; its Washington, DC, headquarters; and other office in the U.S. Its employees in the U.S. and abroad include political appointees as well as career Civil Service and Foreign Service personnel, many of whom are foreign citizens.

The department's threat awareness program is implemented by the Bureau of Diplomatic Security. In the U.S., the Counterintelligence Division of the Office of Investigations and Counterintelligence is responsible for the department's counterintelligence policies and awareness programs. The bureau also chairs the Overseas Security Advisory Council, a joint venture between the department and the U.S. private sector to exchange timely information on security issues relevant to U.S. business.

Overseas, the Bureau of Diplomatic Security's regional security officers (RSOs) protect U.S. personnel and missions overseas; advise U.S. ambassadors on all security matters; and establish and maintain an effective security program against espionage, technical intelligence, terrorist, and criminal threats directed at U.S. diplomatic facilities. The RSO is the focal point for the department's counterintelligence program at post, and is assisted by an interagency Counterintelligence Working Group (CIWG).

The State Department's main counterintelligence mission is defensive in nature: to deter, detect and neutralize foreign intelligence service threats targeted against personnel, technologies and equipment. To implement this, the bureau's foreign intelligence threat awareness program focuses on increasing the awareness of all personnel commensurate with the level of threat they may be exposed to from critical to less critical threats.

The department receives policy guidance from E.O. 12968 *Access to Classified Information* (Aug 4, 1995) and PDD/NSC-12 *Security Awareness and Reporting of Foreign Contacts* (Aug 5, 1993). Of particular importance is 12 FAM 260, *Counterintelligence*. The Omnibus Diplomatic Security And Antiterrorism Act of 1986 outlines the guidelines for the diplomatic security services, but does not discuss counterintelligence issues in any great detail.

The Bureau of Diplomatic Security publishes a semi-annual *Composite Threat List*, which evaluates the HUMINT, TECHINT, terrorist and criminal threats at all overseas facilities staffed by permanently assigned and resident official Americans. Evaluations for the HUMINT and TECHINT portions are conducted by the Overseas Security Policy Board Working Groups on the Human or Technical Intelligence Threats. These working groups are interagency panels comprised of representatives from DS, CIA, DIA, FEB and NSA, working under the chair of the Center for Security Evaluation (CSE). Substantive information concerning the counterintelligence threats at post is shared within the group.

SCOPE

The State Department's counterintelligence program has both domestic and overseas components. Each year, almost 27,000 people receive a Department of State threat awareness briefing. This includes 8,000 employees; 8-10,000 Marine Corps and security guards; and 6,000 contractors. In addition, thousands of Foreign Service National (FSN) employees are also briefed. Others receiving State briefings include employees (including those of other agencies at post), their eligible family members, Seabees, U.S. military attaches and U.S. contractors assigned to our diplomatic establishments, facility visitors, member companies, and business people.

There are 22 employees detailed to the counterintelligence office at State. This includes three analysts and 19 special agents. Two of the agents are assigned as training officers, but are assisted by other office staff. They provide training and develop training materials for the entire department. Other offices provide non-HUMINT security-related awareness training. General defensive briefings are given to all new employees and Civil Service employees whose security clearances have been readjudicated. Special groups are briefed, such as newly assigned Marine Security Guards, as are other agency personnel upon request. Required training is also given to all U.S.-based personnel newly assigned to critical HUMINT threat posts prior to departure for post. The OSAC Committee for Protection of Information and Technology also provides an annual security briefing to some 500 corporate security directors.

The counterintelligence program at overseas missions is commensurate with the post-specific HUMINT threat. The 232 RSOs detailed to 135 diplomatic missions throughout the world provide counterintelligence briefings for all American employees, business people, eligible family members, official visitors, locally hired Americans, and FSNs. At the highest threat posts, refresher briefings are also given.

At critical or high-threat posts, or at posts where there is a changing counterintelligence environment, DS/ICI/CI performs periodic CI Surveys. The survey involves a review of the human intelligence threat at post and an evaluation of the entire counterintelligence program, to include counterintelligence awareness. A comprehensive report is prepared, shared with post management, and distributed to certain outside agencies. In addition, DS/ICI/CI staff members who conduct the surveys will often assist

the RSO by giving briefings to oth American and FSN employees and by participating in other aspects of the awareness program at post.

Records of briefings given to State Department employees are kept in a database. Overseas, RSOs maintain records of briefings given to all Americans at post, Foreign Service Nationals (FSNs), TDYers and visitors for the duration of employment or assignment at post.

PROVIDERS' BACKGROUND AND TRAINING

Domestic providers are special agents and others with strong security backgrounds. The Chief of the Analysis and Special Projects Branch of DS/ICI/CI, the office that oversees the awareness program, is an experienced state certified educator. Domestic providers attend counterintelligence specialized training as well as "train the trainer" courses.

To prepare the RSOs for their counterintelligence role, each completes a comprehensive counterintelligence course provided by the department. The RSO school training includes an intensive 3- or 4-day counterintelligence course given by DS/ICI/CAS and other agency participants which covers all counterintelligence principles and illustrates the use of briefing materials. In addition, counterintelligence basics and special topics are covered during introductory training for special agents and in refresher courses. By law, RSOs assigned to the higher HUMINT threat posts must receive specialized counterintelligence training.

PREPARATION FOR BRIEFINGS

Briefings are conducted in Washington, DC, and at overseas posts. Domestic providers are staff officers from the Division of Counterintelligence and Special Investigations of the Office of Investigations and CI (DS/ICI/CI). They are counterintelligence specialists and can draw upon training, experience and office documentation for appropriate awareness materials. Slides and scripts for the major briefings are available. New materials are produced inhouse as the need arises.

RSOs are provided PowerPoint© outlines for awareness and policy briefings and add post-specific information from the historical record at post or from headquarters officers and analysts. The analysts determine threats at each overseas mission and prepare briefing papers for the department. They work closely with the FBI and CIA, among others. A video which explores recruitment tactcs has been distributed to all RSOs and a new video to supplement the FSN Awareness program is being prepared by DS/ICI/CI and CSE.

RECOMMENDATIONS

Persons interviewed at State offered a number of suggestions for improvements.

Increase funding for conducting CI Surveys which review the human intelligence threat and evaluate counterintelligence programs at critical or high threat posts.

Counterintelligence providers at State Department Headquarters often travel for extended period of time. This increases the demand on the remaining providers to conduct large numbers of required counterintelligence briefings. Additional counterintelligence personnel resources would help to alleviate this situation.

Require all agencies to brief employees destined for overseas travel and assignment in accord with the Foreign Affairs Manual (FAM) provisions.

Appendix F-29

AGENCY	DEPARTMENT OF TREASURY (DOT)
HQ POINT OF CONTACT	Michael L. Romey Special Assistant to Secretary for National Security

BACKGROUND

The Department of the Treasury is the department with the second largest law enforcement resources in the federal government. Its mission is to formulate and recommend economic, fiscal, and tax policies; serve as financial agent of the United States Government; enforce the law; protect the President and other officials; and manufacture coins and currency. Treasury was appointed to the National Foreign Intelligence Board in 1972, thus emphasizing the critical connection between the intelligence community as it has traditionally been defined and those responsible for international economic policy.

The Office of Intelligence Support provides intelligence to the Treasury Secretary and other Department officials. The Office alerts the Secretary and other officials to fast-breaking events, foreign and domestic; obtains intelligence reports and products for Treasury officials; and oversees the intelligence needs of Treasury's offices and bureaus. In addition, the Office participates in the preparation of National Intelligence Estimates and other communitywide intelligence products, developing and coordinating Treasury Department contributions. The Office of Intelligence Support (OIS) consists of 13 employees plus detailees from other intelligence community agencies. This Office is responsible for providing oversight of the Department's intelligence needs and its relationship with the intelligence community. OIS does not have an extensive FITA program, but provides (or arranges for) counterintelligence threat awareness briefings to Treasury officials as required.

The Department of Treasury derives counterintelligence-related policy guidance from E.O. 12333 *US Intelligence Activities* (Dec. 4, 1981); PDD/NSC-12 *Security Awareness and Reporting of Foreign Contacts* (Aug 5, 1993); E.O. 12968 *Access to Classified Information* (Aug 4, 1995); and DCID 1/14 *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information* (Jan 22, 1992). These larger policies are translated into directives and regulations specifically designed for the Department of the Treasury (e.g., *The Treasury Security Manual*).

SCOPE

Most employees at Main Treasury and its bureaus do not require clearances and their nexus with the intelligence world is weak. So Treasury has a very small counterintelligence program directed at its cleared employees. Among the most vulnerable targets are the five Treasury Department Assistant Secretaries, employees within Customs and the ATF, and approximately 40 Headquarters' employees who travel and are exposed to the threat. Employees cleared at the secret level and above receive one-on-one and small group FITA and foreign travel briefings; those cleared at the sensitive compartmented information (SCI) level receive one-on-one and small group indoctrination and security refresher briefings. In addition to these standard briefings, the Treasury Terrorist Advisory Group (TTAG) shares terrorist information with Headquarters' and bureau employees.

Treasury's counterintelligence threat program is primarily focused on employees' vulnerabilities during travel. One-on-one travel briefings are given by a single provider as required whenever subcabinet level appointees and other cleared employees in the Department travel to foreign destinations. Among the most frequent travelers receiving these briefings are the five Deputy Assistant Secretaries. These travel briefings usually provide general guidelines, e.g., current threats to U.S. officials, common sense rules for foreign travel, how to communicate when traveling by using a secure phone. Travelers within each bureau are briefed by their own Security Officers; and the Treasury Secretary is briefed by the Secret Service which is responsible for protecting him and informing him of the foreign intelligence threat.

No system exists for tracking the numbers and types of briefings given at Main Treasury and within the bureaus. However, since very few employees are cleared and only 40 employees at Main Treasury travel on a regular basis, the number of briefings provided annually is relatively small; likewise, small numbers of briefings are assumed to be presented annually within the various bureaus.

PROVIDERS' BACKGROUND AND TRAINING

At Headquarters, a single provider with extensive experience in the intelligence and security field is responsible for developing and presenting all travel and other briefings. This provider has over 10 years of experience being responsible for foreign intelligence threat awareness activities and is well prepared to present effective briefings. This provider reported receiving training in making effective presentations more than seven years ago, but does not require additional training to conduct the counterintelligence program in its current form and level. However, resources aimed at helping local providers obtain and maintain subject matter expertise are needed. Such information would include clear, concise threat background material, sources of threat from the counterintelligence world, canned briefings, etc.

PREPARATION FOR BRIEFINGS

Treasury providers develop their own briefings from scratch and tailor these briefings to some extent to target audiences. For the most part, briefing information is obtained from security publications and from research of intelligence and open source databases. Sources of this information include CIA and NACIC. In addition, canned videos are sometimes obtained from agencies such as NSA for use in initial indoctrination briefings.

RECOMMENDATIONS

Persons interviewed within the Treasury Department offered a number of recommendations for improvements in the FITA program:

There is a need for understanding and differentiating the needs of various organizational cultures within and outside of the intelligence community. This would make it possible for NACIC to produce generic counterintelligence awareness training materials targeted to the different civilian and DoD cultures.

Emphasis should be placed on educating top management and employees of civilian and DoD agencies concerning the changing threat from more traditional military targets to nontraditional economic and technological targets. Since much of the awareness information still focuses on the traditional threat, it is not perceived as relevant to civilian agencies.

NACIC should develop specific information needed by civilian agencies who have neither the budget nor the personnel to dedicate to counterintelligence issues. This information would include details about the threat from specific countries (e.g., sources of the threat, existence of intelligence services or national police forces, modus operandi of the collectors). Such information would help providers at the local level to maintain their subject matter expertise, thus increasing their credibility with their audiences and their effectiveness in presenting counterintelligence information.

APPENDIX G

Data Collection Instruments

Appendix G-1 Questions for Interviewer Guidance for Agency Point of Contact Interviews

Topics:

From your point of view as a policymaker, what topics should ideally be covered in foreign intelligence threat awareness activities in your agency/organization? Are there some topics that should be covered but aren't?

Policies:

What are the major policies that guide the foreign intelligence threat awareness activities in your agency/organization?

Do the policies provide adequate guidance? Are they clear, up-to-date, and sufficient to implement programs? Are they reasonable? How closely does your program correspond to the requirements of the policies? Can we get copies of your directives [if we don't already have them]?

We have tried to get a sense of the general goals for foreign intelligence threat awareness activities, but we are interested in how you see it. Here's our list (C-1). Would you say these were appropriate goals?

Scope:

Please give me an overview of how your program works and how it fits into your agency/organization? A diagram? How is the foreign intelligence threat program communicated to the target populations? Describe the different kinds of briefings and different kinds of audiences (e.g., civilian, military, civilians working for the military, contractors, etc.). How many briefings? How many providers? How often are people briefed? What kind of materials are used (e.g., briefings, videos, pamphlets, etc.)?

What kind of people in the agency/organization are responsible for conducting the foreign intelligence threat awareness program? How are they assigned to this job? Generally, what are the providers' backgrounds? Could you refer us to other points of contact for further information on briefings and materials? We'd eventually like to observe at least one briefing in your agency/organization.

Training of providers:

What are the responsibilities of providers? What guidance on conducting foreign intelligence threat awareness activities is provided to the trainers, if any? Is there any training made available to the providers? If so, what?

Does your agency/organization train employees of other agencies? If so, how many and from what agency? Or do you use other agencies, e.g., DIA or DOE, to conduct briefings in your agency/organization?

Where do you obtain materials for the briefing program (e.g., NACIC)? Could we have a sampling of the CI materials used in your program, such as periodic publications, videos, posters, and other media used for getting the message across?

Impediments/Facilitators:

What factors help or hinder successful foreign intelligence threat activities in your agency/organization?

What are the major problems with the threat awareness activities in your agency/organization? What recommendations would you like to see come out of this study?

Appendix G-2 Foreign Intelligence Threat Information Providers Interview Protocol

Person interviewed:_____

Agency/company:_____

Telephone number:_____

Date of interview:_____

Interviewer:_____

PERSEREC is reviewing foreign intelligence threat awareness programs in the executive branch as part of a study for the National Counterintelligence Policy Board. The goal of the study is to identify ways to enrich these programs. Interviews with those involved with foreign intelligence threat awareness activities are the cornerstone of the study.

We would like to gather from you information about your experience with threat awareness activities; how you prepare threat briefings, including the awareness topics covered; training you may have received to prepare you as a presenter; and your opinions on what could be done to improve foreign intelligence threat awareness activities.

A. Experience and Involvement with Foreign Intelligence Threat Awareness

1. Job title:_____

2. Mailing address:_____

3. If a government civilian employee, what is your GS level?_____

4. If a uniformed member of military, what is your rank?_____
   (Officers, 01-10; Enlisted, E4-E9; Warrant/LDO)

5. Which of the following best describes the primary responsibilities of your current position?

a. counterintelligence
b. intelligence
c. security
d. law enforcement
e. other_____

6. Including the time in your current position, how many years in your entire career have you had some responsibility for foreign intelligence threat awareness activities? _____years.

7. In your current position, what percentage of your time is spent preparing and delivering foreign intelligence threat awareness information?

a. <20
b. 20-39
c. 40-59
d. 60-79
e. >79

B. Types of Audiences, Briefings and Printed Materials

Describe the types of target audiences for the foreign intelligence threat awareness briefings and printed materials that you have developed during the last 12 months. Include the occupational or functional specialty that describes the target audiences, their seniority, degree of homogeneity, and the reasons that the audiences are being briefed.

_____
_____
_____
_____
_____

2. To what extent do you emphasize foreign intelligence threat awareness information in each of the following?

Rating scale	Type of briefing/printed material
1 = not at all	_____foreign intelligence threat awareness
2 = to a small extent	_____initial security indoctrination
3 = to some extent	_____security refresher
4 = to a great extent	_____foreign travel
5 = to a very great extent	_____printed materials (e.g., brochures)
N/A	_____other_____

3. How many people typically attend each of the following types of briefings or receive printed materials that you provide?

Number of People	*Type of briefing/printed materials*
a. <5	_____foreign intelligence threat awareness
b. 5-10	_____initial security indoctrination
c. 11-25	_____security refresher
d. 26-75	_____foreign travel
e. >75	_____printed materials (e.g., brochures)
N/A	_____other_____

4. Typically, what is the classification level of the briefings that you provide?

Classification level	*Type of briefing*
a. unclassified	_____foreign intelligence threat awareness
b. confidential	_____initial security indoctrination
c. secret	_____security refresher
d. top secret	_____foreign travel
e. sensitive compartmented information (SCI)	_____other_____

5. If the response to item 4 is "unclassified," could your briefings have been more effective if you had the opportunity to present classified information?

If yes, explain_____

_____

_____

_____

6. If the response to item 4 is "confidential," "secret," "top secret," or "SCI," could you have been as effective presenting the message in an unclassified setting?

If yes, explain_____

_____

_____

_____

C. Developing Briefings and Printed Materials

1. To what extent do you rely on the following?

Rating scale	*Type of material*
1 = not at all	_____canned briefings developed by someone else
2 = to a small extent	_____briefings you develop from scratch
3 = to some extent	_____other_____
4 = to a great extent	_____
5 = to a very great extent	
N/A	

2. If you rely on canned briefings, where do you obtain them?_____

3. To what extent do you tailor briefings for particular target audiences?

1 = not at all
2 = to a small extent
3 = to some extent
4 = to a great extent
5 = to a very great extent
N/A

4. If response to item 3 is "not at all," "to a small extent," or "to some extent," list the reasons more effort is not made to tailor briefings.

_____

_____

_____

5. If you do develop your own briefings or printed materials, to what extent do you use the following types of background information?

Rating scale	*Type of background information*
1 = not at all	_____newspaper articles
2 = to a small extent	_____databases
3 = to some extent	_____security seminars
4 = to a great extent	_____security publications
5 = to a very great extent	_____other _____
N/A	

6. For briefings or printed materials that you develop, indicate whether you use each of the following sources of information. For each source, indicate the quality and availability of the products and services. Please use the scales in the box below.

	Rating scales
use	*quality and availability*
y = yes n = no	1. poor 2. below average 3. average 4. above average 5. excellent

	Source Availability	*Use*	*Quality*
a. other parts of my own organization/ agency	_____	_____	_____
b. other intelligence, CI or security managers in my organization/agency	_____	_____	_____
c. National Counterintelligence Center	_____	_____	_____
d. Department of Defense Security Institute	_____	_____	_____
e. National Security Agency	_____	_____	_____
f. FBI's ANSIR (old DECA) program	_____	_____	_____
g. Overseas Advisory Council	_____	_____	_____
h. National Reconnaissance Organization	_____	_____	_____
i. Department of Energy	_____	_____	_____
j. CIA	_____	_____	_____
k. Defense Investigative Service	_____	_____	_____
l. Non-government security organizations	_____	_____	_____
m. other, specify_____			
_____	_____	_____	_____

7. Do you establish specific learning objectives for your foreign intelligence threat awareness briefings?

_____ Yes. How do you decide which learning objectives to include. Are they written?

_____

_____

_____

_____No. Why are formal objectives not developed?

_____

_____

_____

_____

D. Topics Covered in Foreign Intelligence Threat Awareness Briefings and Printed Materials

1. How do you decide on the topics to cover in briefings or printed materials?

_____

_____

_____

_____

2. In the next set of questions, we are interested in FITA topics:

a. Sources of the threat
b. Modus operandi of foreign intelligence agents, services and collectors
c. Types of information being targeted
d. The insider threat and volunteer spies
e. Personnel security indicators and vulnerabilities
f. The technical and non-HUMINT threat
g. Consequences of espionage for the nation and for the offender
h. Special vulnerabilities during foreign travel
i. Espionage case studies
j. Response to the threat: the threat and security countermeasures

For each of these topics, we are interested in the following issues:

- Is the topic addressed in briefings or printed materials?
- If the topic is addressed, what specific information is presented?
- Are sample materials which address the topic available (e.g., briefing slides, brochures, scripts, etc.)?
- Are you able to cover the topic adequately? If not, why?

E. Methods of Presenting Foreign Intelligence Threat Awareness Information

1. Indicate how often you use the following training methods to present foreign intelligence threat awareness information.

Rating scale	*Method type*
1 = never	_____formal standup briefings (group < 50)
2 = seldom	_____formal standup briefings (group > = 50)
3 = sometimes	_____one-on-one or small groups of rank and file
4 = often	_____one-on-one or small groups of middle managers
5 = always	_____one-on-one individual or small groups of executives
N/A	_____seminars or discussion groups
	_____reading material
	_____computer-based training on LAN or diskette

2. Indicate how often you use the following types of media in support of live presentations of foreign intelligence threat information.

Rating scale	*Media type*
1 = never	_____viewgraphs, 35mm slides or computer slide show
2 = seldom	_____slide show with audio
3 = sometimes	_____government produced videos
4 = often	_____commercially produced videos
5 = always	_____internally produced videos
N/A	_____guest experts
	_____externally developed posters & other visual reminders
	_____handouts such as memos, bulletins, newsletters, reference materials, or brochures
	_____other, specify_____
	_____

3. Of the media types checked in question 2 above, which ones do you find to be:

a. Most useful, and why? _____

_____

_____

_____

_____

b. Least useful, and why?_____

_____

_____

_____

_____

F. Subject Matter Expertise and Presentation Skills

1. Do you feel that you have sufficient subject matter expertise to effectively communicate foreign intelligence threat awareness information?

_____ Yes.

_____ No. On what subjects do you require greater information?_____

_____

2. Assess the extent to which you feel well prepared to do the following:

Rating scale
1 = not at all
2 = to a small extent
3 = to some extent
4 = to a great extent
5 = to a very great extent

Presentation Skills
_____design effective presentations
_____design effective audio/visual aids
_____speak before an audience
_____keep audience attention
_____project professional credibility regarding foreign intelligence threat
_____bring "routine" material alive
_____be well received by senior level audiences
_____find resources needed to develop or deliver foreign intelligence threat awareness information
_____develop printed materials

G. Training Opportunities

1. How many years ago did you receive training to help you make effective presentations?

   a. < 1
   b. 1-3
   c. 4-7
   d. > 7
   e. never

2. If you have received training, please list below the courses attended and rate their quality and value using the definitions and scales in the box below.

Rating scale	*Definitions*
1. poor 2. below average 3. average 4. above average 5. excellent	Quality = extent to which the training is conceptually sound, well-designed and uses well-integrated training methods and instructional aids Value = extent to which you found the training relevant to fulfilling your job responsibilities

Courses attended	*Quality*	*Value*
a._____	_____	_____
b._____	_____	_____
c._____	_____	_____
d._____	_____	_____

3. Would additional training help you to be significantly more effective in disseminating foreign intelligence threat awareness information?

   _____ If yes, what courses do you want to take, or on what subjects do you need training?

_____

_____

_____

_____

H. Overall Assessment

1. Describe three factors that lead you to successfully disseminate foreign intelligence threat awareness information in your organization. Please list in order of priority.

_____

_____

_____

_____

_____

2. Describe up to three obstacles to the effective dissemination of foreign intelligence threat awareness information in your organization. Please order them by degree of seriousness.

_____

_____

_____

_____

_____

3. Please suggest three things that could be done to improve your dissemination of foreign intelligence threat awareness information in your organization/agency, in order of priority. Who do you think should take action?

_____

_____

_____

_____

_____

4. Please describe three lessons that you have learned, that you would like to pass on to others charged with disseminating foreign intelligence threat awareness information.

_____

_____

_____

5. What could the government do to help improve the way foreign intelligence threat information is disseminated in the government?

Appendix G-3 Audience Survey

LEAVE BLANK
Agency _____
Type of Briefing _____

The Defense Personnel Security Research Center (PERSEREC) is reviewing foreign intelligence threat awareness programs in the executive branch as part of a study for the National Counterintelligence Policy Board. The goal of the study is to identify ways to improve current foreign intelligence threat awareness programs. A cornerstone of this study is evaluations of the foreign intelligence threat awareness briefings by recipients likely yourself. Your responses to this survey are anonymous.

Indicate the extent to which you agree or disagree with each of the following statements using the scale below. Place the appropriate number in the space before each statement.

1	*2*	*3*	*4*	*5*
strongly disagree	*disagree*	*neither agree nor disagree*	*agree*	*strongly agree*

The briefing as a whole (including the format, content, media used, and presenter) :

_____ 1. Made a convincing case that foreign intelligence activity, including espionage by insiders, is a serious concern that affects us all, and is not an imaginary threat.

_____ 2. Clearly spelled out indicators of possible foreign intelligence interest or activity.

_____ 3. Specifically described the types of situations in which I might be a target of foreign intelligence activities.

_____ 4. Clearly defined how my own behavior, especially while in foreign countries, may unintentionally attract foreign intelligence interest.

_____ 5. Explicitly advised me of my obligation to report suspicious or improper activity to appropriate authorities, and to whom to report it.

_____ 6. Covered specific examples of suspicious or improper activity.

_____ 7. Made a convincing case to report to officials any incidents of security concern that I might observe in the future.

_____ 8. Will help deter individuals from committing espionage or other deliberate security breaches.

_____ 9. Had clear objectives.

_____ 10. Was credible.

_____ 11. Was well-prepared.

_____ 12. Was presented in an interesting fashion.

_____ 13. Used aids (e.g., videos, handouts, posters) that were very good.

_____ 14. Was relevant to me in terms of my job.

15. Considering both the content and effectiveness of the presentation, rate the briefing overall. *Place a (✓) in the space before the rating.*

_____ Excellent

_____ Above Average

_____ Average

_____ Below Average

_____ Poor

16. Please provide comments summarizing what you consider to be the most and least effective aspects of the briefing.

_____

_____

_____

_____

_____

17. Please indicate your rank/grade: _____

Thank you for completing this survey.

Appendix G-4 Focus Group Protocol

PURPOSE, GROUP SIZE, SELECTION CRITERIA, MEETING TIME AND ROLES

Purpose. The purpose of the focus group is to obtain audience reactions to the content and presentation style of the briefing. We are attempting to glean insights into what makes for an effective foreign intelligence threat briefing. Specific examples and anecdotes of what captures and holds the attention of the audience are the stuff we are looking for in this exercise.

Type of Briefing Selected. Focus groups should be conducted following the more generic FITA briefings or refresher briefings with larger audiences. If possible, avoid having to conduct a focus group following a very specific briefing with a limited number of participants, (e.g., travel briefing or specialized small group briefing).

Group Size. Each focus group should be comprised of 7, plus or minus 2, participants. Allowing for absentees, at least 7 participants should be selected prior to the briefing.

Selection Criteria. To the extent possible, the POC or Provider should be given an explicit set of criteria for selecting group members in advance of the briefing. This will allow the group members to plan their schedules so they can participate in the focus group. The selection criteria should be followed as closely as possible and should include the following:

- Include a cross-section of employees who will be attending the briefing. These employees should represent the various units/bureaus/services, etc. within the agency.
- Include individuals with different types of skills (e.g., administrative types, management types, scientists/researchers, line managers, etc.).
- Avoid selecting individuals who work for one another (e.g., a supervisor and his/her subordinates).
- In selecting group members, rank is important. If possible, try not to mix higher ranking individuals with much lower ranking individuals. That is, avoid mixing high and mid-level managers with non-supervisory employees in the same group.

In cases where the attendees are not known in advance, an alternative strategy should be developed in cooperation with the POC or Provider. If no other alternative exists, volunteers may be sought from the audience.

Meeting Time. The focus group should start as soon as possible after the briefing, allowing time for only a quick break between the sessions. The focus group session should last approximately 1 - 1.5 hours and be conducted in a meeting place that is quiet, comfortable and private. If possible, the room should be arranged so that the participants sit facing one another around a conference table; if not, rearrange the room so the chairs are in a circle, creating an atmosphere conducive to discussion.

Roles. There will be two facilitators: one has the role of leader who will do most of the talking. The other facilitator will observe and record the proceedings. This person may support the leader by offering occasional observations or suggestions. But the first facilitator should be clearly viewed as the leader of the group.

OPENING

Introductions. The leader should open the focus group by making introductions and thanking participants for taking the time to help in the endeavor. Ask the participants to go around the room briefly introducing themselves by giving their first name, job title, and service/department/bureau.

Explain Purpose of Session. The leader should explain why the facilitators are conducting the session and why the participants have been asked to participate.

1. *Why is the session being conducted?* PERSEREC, a government research facility, has been asked by the NACIPB to review foreign intelligence threat awareness programs in the executive branch. The goal of the study is to identify ways to improve current foreign intelligence threat awareness programs.

2. *Why are the participants there?* A cornerstone of the study is evaluations of foreign intelligence threat awareness briefings by recipients of same. The goal of doing these briefings is to inform and assist people like themselves. Since they are the intended audience for these briefings, we want get their views on the value of the experience. They are the key - if they are not getting something from the experience, the whole focus group exercise is a waste of time.

Mention that we are conducting focus groups with people like themselves in over 30 agencies within the Executive Branch and that they have been selected to represent different areas or specialties within their agency.

Definition and Ground Rules for a Focus Group. Explain what a focus group is and what is expected of the group members by saying the following:

"There are a few ground rules associated with focus groups. First, the term "focus group" is just another way of saying we're going to have a group discussion. We will ask you to focus on various topics and would appreciate hearing your honest opinions. We want to hear all your ideas, opinions, and comments.

The most important ground rule is that there are no right or wrong answers. Please feel free to say what's on your mind. If you don't agree with someone else who's talking, please speak up when they have completed their thought. We want to hear from all of you.

Concrete examples are especially helpful in our discussions, but please do <u>no</u>t use any actual names.

Everything you say in this room is confidential. You will never be identified with anything you say. Some of your responses may be quoted in our reports, but we will never use your names, or other identifying information. We also request that you not repeat anything that is said today outside of this group."

How the Focus Group Works. So group members are not surprised, mention the following:

"_____ is taking notes during the group to help us remember the points you make. He/she will not be associating names or titles with these comments.

Since time is limited, I may have to cut you off occasionally to move on to a new topic."

How the Group Discussion Will Work. The leader will explain that the members of the group will discuss the briefing they just observed in the context of eight objectives for threat awareness activities. Each objective will be explained and discussed in turn. The members of the group will be asked whether they agree (or not) that the objective was achieved. (Note to facilitators: do not press members who cannot decide).

The group will discuss why or why not each objective was achieved. If members thought that the objective was met (agreed), they will explain what the presenter did to be successful. If members thought that the objective was not met (disagreed), they will explain what the presenter did that precluded success. Members also will be asked to indicate what the presenter could (or should) have done to be successful. The leader will encourage group members to provide concrete examples and anecdotes in their explanations.

The facilitator will use a flip chart to guide and record the discussion. The objective to be addressed will be printed on the top of a sheet on the flip chart . The facilitator will explain the objective using specific questions in the "List of Objectives" section below. The proceedings will be recorded in the appropriate areas of the flip chart (see sample flip chart below). The facilitator will proceed through flip chart sheets, one for each of the eight objectives.

Close by offering an opportunity for group members to add any further comments or suggestions about the briefing that caused it to be successful (or not), as the case may be. Thank participants for cooperation in this important task. Explain that results of the focus groups will be put together with information collected from a variety of sources (providers, policymakers, audiences across executive branch). Results will be reported to NACIPB in August.

List of Objectives

1. Threat Existence. Did the briefing convince you that foreign intelligence activities exist, are a serious concern, and are not just an imaginary threat?

2. Threat Signals. Did the briefing help you recognize indicators of possible foreign intelligence interest or activity? Which examples of suspicious or improper activity were most helpful?

3. Targeting. Did the briefing help you understand the types of situations in which you might be targeted? Did it show you how your own behavior may unintentionally attract foreign intelligence interest, especially in foreign countries?

4. Reporting. Were you convinced to report incidents of security concern? Was your obligation to do so made clear, as well as the procedures for reporting such activities?

5. Deterrence. Do you believe that the briefing will help deter individuals from committing espionage or other deliberate security breaches?

6. Relevance. Was the briefing relevant to your job?

7. Provider. What was your overall evaluation of the provider? Was the provider credible? Well-prepared?

8. Overall Briefing. What was your reaction to the briefing as a whole? Did the briefing have clear objectives? Was it interesting? Were the aids used in the presentation very good or effective?

Sample Flip Chart

THREAT EXISTENCE

_____Agree _____Disagree

Why?	**Why not?**

Could (should) have done?

Appendix G-5 Briefing Observation Form

Briefing Observation Form
Foreign Intelligence Threat Awareness Project

Descriptive Information

Sponsoring Agency: Briefer's Name:

Briefing Location: Briefer's Agency:

Briefing Date: Observer's Name:

Audience Characteristics

Size: Occupational Specialty:

Seniority: Reason for Briefing:

Type of Briefing, Method of Presentation, and Media Used

Type of briefing:

_____ Foreign intelligence threat awareness
_____ Initial security indoctrination
_____ Security refresher
_____ Foreign travel
_____ Other, specify _____

Method of presentation (more than one may be checked)

_____ Formal standup briefing
_____ Other, specify _____

Media used (more than one may be checked)

_____ Viewgraphs _____ 35mm slides _____ Computer slide show
_____ Slide show with audio _____ Video _____ Guest experts
_____ Posters/visual reminders _____ Newspapers
_____ Handouts (e.g., memos, bulletins, newsletters, reference materials, brochures, etc.)
_____ Other, specify_____

Learning Objectives - Using the three-point scale below, assess the extent to which there was an attempt to address each of the following objectives:

1 = great extent *2 = some extent* *3 = not at all*

____ Convince individuals that foreign intelligence activity, including espionage by insiders, is a serious concern that affects us all, and is not an imaginary threat.

____ Help individuals recognize indicators of possible foreign intelligence interest or activity.

____ Sensitize individuals to the types of situations in which they might be targets of foreign intelligence activities.

____ Sensitize individuals to the ways in which their behavior, especially while in foreign countries, may unintentionally attract foreign intelligence interest.

____ Inform individuals of their obligation to report suspicious or improper activity to appropriate authorities, and to whom to report it.

____ Describe specific examples of suspicious or improper activity that should be reported.

____ Persuade individuals to report to officials any incidents of security concern that they might observe in the future.

____ Deter individuals from committing espionage or other deliberate security breaches.

Briefing Content - Using the three-point scale below, assess the extent to which the briefing covered each of the following topics (in bold). Place a (✓) next to the statements under each topic that were addressed.

1 = emphasized *2 = mentioned* *3 = not covered at all*

_____**Sources of the threat.**

(✓)
_____Examples of countries involved in intelligence operations against US interests.

_____Case examples(s) of "friendly" countries involved in intelligence operations against U.S. interests.

_____Examples of threats to U.S. information from non-state entities such as R.s.ian and other foreign organized crime, terrorist groups and foreign companies.

_____**Modus operandi of foreign intelligence agents and services, and collectors.**

(✓)
_____Description of techniques for eliciting information.

_____Definition and case study examples of ethnic targeting.

_____Caution to limit discussions of one's work with foreign representatives.

_____**Types of information being targeted.**

(✓)
_____Review of high-priority targets (e.g., based on National Security Threat List, NSTL).

_____Review of specific technologies which have been targeted and evidence of this.

_____Outline the current interest in dual-use and economically significant technology.

_____**Insider threat and volunteer spies.**

(✓)

_____Documentation that most espionage is committed by volunteers.

_____Review of causes of volunteer espionage (e.g., financial problems, alcohol abuse).

_____Identification of presumed motivations of known offenders (e.g., financial need or greed).

_____**Personnel security indicators.**

(✓)

_____Informed target audience of its obligation to report any suspicious or improper activity by *outsiders*, and to whom.

_____Informed target audience of its obligation to report any suspicious or improper activity by *insiders*, and to whom.

_____Review of specific examples of suspicious or improper activity that should be reported.

_____**Technical and non-HUMINT threat.**

(✓)

_____Discuss the intelligence targeting of encrypted voice, fax and data communications.

_____Review current threat to restricted information systems and computer networks posed by hackers.

_____Review the technical threat and reasonable countermeasures to minimize electronic eavesdropping.

_____Review and define other non-HUMINT intelligence collection methods (IMINT, SIGINT, etc.).

_____**Consequences of espionage for nation.**

(✓)

_____Specifics about damage or potential damage from recent espionage cases, quoting media or open sources.

_____Concrete information from classified or non-open official sources about damage incurred by loss of information, if sanitized.

_____Types of damage possible from espionage: loss of life, intelligence systems, diplomatic negotiating strength, military advantage, economic opportunities.

_____**Vulnerabilities during foreign travel.**

(✓)

_____Discussion of technical surveillance measures directed at U.S. citizens abroad.

_____Examples of targeting of U.S. citizens, even in "friendly" countries.

_____Examples of covert search and theft or compromise of classified or proprietary materials while en route or at hotels.

_____General guidelines for the U.S. traveler at a foreign location to counter espionage threat.

_____**Consequences of espionage for offender, family and friends.**

(✓)

_____Use of case examples to portray the level of despair and suffering by persons directly or indirectly involved with espionage.

_____Cite case studies which illustrate severity of imprisonment in serious cases.

_____**Threat and security countermeasures.**

(✓)

_____Explain the rationale for security countermeasures in terms of specific threat information.

_____Show how lessons learned from specific cases have led to the adoption of security countermeasures.

Presentation Evaluation - Using the three-point scale below, assess the degree to which you agree or disagree with each of the following statements:

1 = Agree *2 = Neither agree nor disagree* *3 = Disagree*

____ Objectives clearly stated or implied in the content of the briefing.

____ References were made to recent espionage cases to illustrate one or more points in the presentation.

____ Information was provided about new policy, legislation or implementation of countermeasures.

____ Briefing was presented in an interesting fashion.

____ Motivational content was tailored to the age and occupational status of the audience.

____ The message reinforced the idea that most people are loyal and responsible.

____ Message de-glamorized the supposedly romantic aspects of espionage.

____ Audience appeared to pay close attention to the speaker during the briefing.

____ Briefing made a convincing case for the reality of current threat.

____ Presenter was a credible source of information.

____ Presenter cited authoritative sources.

____ Materials used in the presentation were very good (e.g., videos, handouts, briefing aids, etc.)

____ Presenter provided sufficient opportunity for questions.

____ Presenter provided good answers to questions asked.

Overall Evaluation - Assess the overall briefing, considering both the content and the effectiveness of the presentation.

____ Excellent

____ Above Average

____ Average

____ Below Average

____ Poor

List specific strong points that made the briefing effective:

List specific weak points that made the briefing ineffective:

Additional comments: See attached briefing notes.

Appendix G-6 Sample Materials Evaluation Form

1. Item number_____

2. Type of item.

   a. video/35mm slides

   b. conference agenda/course syllabus

   c. briefing

   d. newsletter

   e. brochure/pamplet

   f. other_____

3. Classification level.

   a. classified

   b. unclassified

4. Produced by._____

5. Topics covered in the sample (✓) those that apply).

   _____Sources of the threat.
   _____Modus operandi of foreign intelligence agents and services, and collectors.
   _____Types of information being targeted.
   _____Insider threat and volunteer spies.
   _____Personnel security indicators.
   _____Technical and non-HUMINT threat.
   _____Consequences of espionage for nation.
   _____Vulnerabilities during foreign travel.
   _____Consequences of espionage for offender, family and friends.
   _____Threat and security countermeasures.
   _____Other_____

   _____

6. The quality of the content in the item is:

    a. high

    b. average

    c. poor

7. The presentation quality of the information in the item is:

    a. high

    b. average

    c. poor

8. Would it be appropriate to disseminate this item widely across government agencies?

    a. yes

    b. no

9. Would it be appropriate to disseminate this item to government contractors?

    a. yes

    b. no

10. Comments.

_____

Appendix G-7 Industry Providers of Foreign Intelligence Threat Information Telephone Protocol

Person Interviewed: _____ **Date:** _____

Company: _____ **Interviewer:** _____

Phone Number: _____ **Fax number:** _____

As you are aware, PERSEREC is reviewing foreign intelligence threat awareness programs as part of a study for the National Counterintelligence Policy Board. The goal of the study is to identify ways to enrich these programs. Talking to those actually involved with foreign intelligence threat awareness activities is the cornerstone of the study. We'd like to get some notion from you of how the foreign intelligence threat is communicated in your company.

A couple of preliminary questions. Can you tell me the number of employees at your facility?

What is the classification level of the work you do? SAP? Classified? Proprietary? Mixed? (Then decide with the interviewee which level to discuss in the interview.)

Who is your company doing work for? Government? Private sector? If government, which agencies?

[Find out if interviewee is an actual presenter him/herself, or simply a senior manager.] Do you yourself give briefings?

A. Types of Audiences, Briefings and Printed Materials

Who is your audience?

What method do you use to communicate the threat to your audience? (To include type of briefing, size of audience, use of videos, etc.)

What media do you find the most and least useful?

B. Developing Briefings and Materials

Where do you obtain information for your briefings?

Of the sources of information you have mentioned, how would you rank the quality and availability of the information?

C. Briefing Topics

[Mention the topic check list that summarizes topics generally covered in threat awareness activities. Ask if interviewee would be willing to fill it out and FAX it back to us (to save telephone time.)]

Do you have any sample briefing materials? Could you share copies with us? [Mention we are looking for *excellence*.]

D. Subject Matter Expertise and Presentation Skills

[If the interviewee is a briefer, ask one general question about his/her subject-matter expertise and presentation skills.]

E. Overall Assessment

This is the one big open-ended question where "the industry point of view can be reflected," the words we used in our intro letter. So we're looking for problems, and suggested solutions.

Describe obstacles to the effective dissemination of foreign intelligence threat awareness information.

Suggest things that could be done to improve your dissemination of foreign intelligence threat awareness information and who should take the action (industry, government)?

[Thank the interviewee, and remind about filling out topic check list which will be faxed to him/her the same day as interview.]

Appendix G-8 Topic Evaluation Form for Industry Representatives

Please be kind enough to fill in the questionnaire, along with the identifiers on the bottom of page 2, and fax to PERSEREC (Jim Riedel) at (408) 656-2041 or (408) 656-5050.

Using the three-point scale below, assess the extent to which threat awareness activities in your facility address each of the following topics (in bold). Place a (✓) next to the statements under each topic that your awareness activities address.

1 = emphasized *2 = mentioned* *3 = not covered at all*

_____**Sources of the threat.**

(✓)

_____Examples of countries involved in intelligence operations against U.S. interests.

_____Case examples(s) of "friendly" countries involved in intelligence operations against U.S. interests.

_____Examples of threats to U.S. information from non-state entities such as Russian and other foreign organized crime, terrorist groups and foreign companies.

_____**Modus operandi of foreign intelligence agents and services, and collectors.**

(✓)

_____Description of techniques for eliciting information.

_____Definition and case study examples of ethnic targeting.

_____Caution to limit discussions of one's work with foreign representatives.

_____**Types of information being targeted.**

(✓)

_____Review of high-priority targets (e.g., based on National Security Threat List, NSTL).

_____Review of specific technologies which have been targeted, and evidence of this.

_____Outline the current interest in dual-use and economically significant technology.

_____**Insider threat and volunteer spies.**

(✓)

_____Documentation that most espionage is committed by volunteers.

_____Review of causes of volunteer espionage (e.g., financial problems, alcohol abuse).

_____Identification of presumed motivations of known offenders (e.g., financial need or greed).

_____**Personnel security indicators.**

(✓)

_____Informed target audience of its obligation to report any suspicious or improper activity by *outsiders*, and to whom.

_____Informed target audience of its obligation to report any suspicious or improper activity by *insiders*, and to whom.

_____Review of specific examples of suspicious or improper activity that should be reported.

_____**Technical and non-HUMINT threat.**

(✓)

_____Discuss the intelligence targeting of encrypted voice, fax and data communications.

_____Review current threat to restricted information systems and computer networks posed by hackers.

_____Review the technical threat and reasonable countermeasures to minimize electronic eavesdropping.

_____Review and define other non-HUMINT intelligence collection methods (IMINT, SIGINT, etc.).

_____**Consequences of espionage for nation.**

(✓)

_____Specifics about damage or potential damage from recent espionage cases, quoting media or open sources.

_____Concrete information from classified or non-open official sources about damage incurred by loss of information, if sanitized.

_____Types of damage possible from espionage: loss of life, intelligence systems, diplomatic negotiating strength, military advantage, economic opportunities.

_____**Vulnerabilities during foreign travel.**

(✓)

_____Discussion of technical surveillance measures directed at U.S. citizens abroad.

_____Examples of targeting of U.S. citizens, even in "friendly" countries.

_____Examples of covert search and theft or compromise of classified or proprietary materials while en route or at hotels.

_____General guidelines for the U.S. traveler at a foreign location to counter espionage threat.

_____**Consequences of espionage for offender, family and friends.**

(✓)

_____Use of case examples to portray the level of despair and suffering by persons directly or indirectly involved with espionage.

_____Cite case studies which illustrate severity of imprisonment in serious cases.

_____**Threat and security countermeasures.**

(✓)

_____Explain the rationale for security countermeasures in terms of specific threat information.

_____Show how lessons learned from specific cases have led to the adoption of security countermeasures.

Name:_____

Company:_____