

Submitted to
Protection Technology Hanford
and
Fluor Hanford
May 9, 2001



Hanford Security

Conducted by

Washington State
University

Consumer Behavior
Students

Kevin Higginson
Alison Marcum
Sophia Orozco
Dennis Walters

Directed by
Pamela Henderson, Ph.D.

A Perceptual Research Study
on
Security Awareness and Ownership
at Hanford

Executive Summary

Protection Technology Hanford (PTH) in conjunction with Fluor Hanford (FH) and the Department of Energy Richland Operations (DOE-RL) requested a program and Perceptual Research study be conducted by Washington State University (WSU) to assess employee awareness of communications regarding, and commitment to, procedures and guidelines of its current Security Education and Awareness Program (SEAP). This study was done as part of a Consumer Behavior course under the direction of Dr. Pamela Henderson, Associate Professor, in WSU's marketing program.

Mr. Chester Braswell, Security Awareness Coordinator, is responsible for promoting security awareness and ownership among FH employees at the Hanford site, and has overseen the study from its inception. The study was intended to assist Mr. Braswell in determining how to use limited resources effectively to maximize security awareness and ownership at Hanford. In general, we attempted to learn what should be communicated in order to motivate employee commitment to security, and how it should be communicated to be most effective.

The bulk of our research involved conducting in-depth interviews with individuals in three specific segments: security managers at Hanford (and related sites), TRADE representatives from other DOE sites, and mid-level managers at Hanford. Alison Marcum and Sophia Orozco were also given the opportunity to travel to Washington, D.C. to attend the annual Security Education Special Interest Group conference, held in Arlington, Virginia.

It is apparent that people know, cognitively, the importance of security regardless of the level of commitment they demonstrate. Managers do not feel that they would face consequences if their employees do not comply. Badging, protection of classified/sensitive information, and the protection of special materials were thought to be the most important security issues. Little value was seen in stressing "blanket procedures" that do not apply to everyone. Specifically, the most successful elements of the security program were perceived to be audits, patrols, and reports. Managers identified problems/frustrations as difficulty in understanding security expectations and why certain policies are in place.

From our findings we developed a number of enhancements that if implemented, could increase employee levels of awareness and ownership for security.

TABLE OF CONTENTS

I. Introduction	1
II. Purpose	3
III. Methodology	4
IV. Competitor Analysis	6
a. Competitive Environment	6
b. Case Study	8
V. Industry Analysis	22
VI. Customer Analysis	28
VII. Content Analysis	34
VIII. Recommendations & Implementation	65
IX. Actions	77
X. Appendices	
Appendix A	
Elements of Security Awareness Culture	A. 1
Expert Interviews	A. 4
Offsite Interviews	A. 13
Hanford Management Interviews	A. 24
Hanford Standards of Conduct	A. 60
Appendix B	
SE SIG Interviews	B. 1
Appendix C	
Competitor Analysis/Case Study Tables	C. 1
Supporting Literature	C. 9
Appendix D	
Recommendation Samples	D. 1

Introduction

Background

The primary goal of a security program is to create an alert, actively involved workforce to reduce security related incidents. Employee perceptions about the program's significance play an important role in their individual levels of commitment to the program. Since the early 1990s, when the focus of the Hanford site shifted from production of nuclear materials to environmental restoration, perceptions as to the importance of security are believed to have changed. Issues that involve national security are no longer an everyday concern for all employees as they once were, resulting in an apparent change to the level of their commitment to the security awareness program.

Protection Technology Hanford (PTH) in conjunction with Fluor Hanford (FH) and the Department of Energy Richland Operations (RL) requested that a program and Perceptual Research study be conducted to assess employee awareness of communications regarding, and commitment to, procedures and guidelines of its current Security Education and Awareness Program (SEAP). The program's ultimate goal is to reduce security incidents by creating a "vibrant security culture" in which individuals are committed to supporting the security program. Changing the culture of a particular organization begins at various levels of management and is made up of a combination of elements, including but not limited to:

- In-depth training
- Effective communication tools
- Motivation
- Active participation
- Leadership – Example set by management
- Performance measurement

Current Practices

Currently the Security Education and Awareness Program uses a number of practices and tools to gain and maintain security awareness and ownership. The most widely sought after awareness tool is that the Security "ED" cartoons. These cartoons are published in the Hanford Reach on a regular basis, in which the "ED" character discusses and gives pointers about how to improve and maintain a security-minded workforce. Web banners, another frequently used method of communication, allow employees to easily access and review security related topics through Hanford's area network. Other popular tools used to strengthen awareness and ownership include posters, an employee recognition program ("Security Pays in Many Ways"), and periodic security presentations, all of which have been used with some amount of success.

Participants

To gain valuable research experience while participating in a project of great real-world importance, we conducted this study as part of a Consumer Behavior course in Washington State University's marketing program. Dr. Pamela Henderson, Associate Professor at WSU, was responsible for project oversight as well as for providing guidance during each phase of the study. Studying consumer behavior is an integral part of market research, and is an appropriate discipline with which to approach this project. Determining those things that motivate commitment within a group of individuals helps to appropriately tailor communications to the group.

Chester Braswell, Security Awareness Coordinator, is responsible for promoting security awareness and ownership among employees at the Hanford site, and has overseen the study from its inception. Mr. Braswell is responsible for handling new employee security training, communicating updates of program initiatives, and building employee awareness and ownership of security and its importance. This study is intended to assist Mr. Braswell in determining how to use limited resources most effectively to maximize security awareness and ownership at Hanford.

Purpose

Goals

We conducted an in-depth study of managerial perceptions about Hanford's Security Education and Awareness Program in order to reach the following goals:

- Determine the strengths and weaknesses of the current Security Education and Awareness Program from a communications standpoint
- Recommend how the current Security Education and Awareness Program might be enhanced to broaden its appeal and to improve Project Hanford employee participation in program initiatives
- Establish a baseline of information that will provide measurements and meaningful conclusions so that management can then target specific areas for program emphasis

Overall, we were attempting to learn what should be communicated in order to motivate employee commitment to security, and how it should be communicated to be most effective.

Methodology

Market Segmentation

In order to accomplish our goals, we divided the population studied into three segments and addressed questions appropriate to each segment. The segments are as follows:

Security Managers at Hanford (and related DOE sites)

The interview process for this group of individuals involved conducting a brainstorming session in which managers were asked to identify their perceptions regarding the key elements of an outstanding security culture. These sessions were facilitated using the “Fuzzy Performance Indicator Process” as a guideline. A complete diagram of this process is located in Appendix A.

In using this brainstorming process, we were attempting to develop a prioritized “list” of elements that would collectively indicate the characteristics of a vibrant security culture.

TRADE Representatives from Other DOE Sites

The intention of these interviews was to find out what kinds of things were being implemented at sites other than Hanford, and identifying those that appeared to be most successful in encouraging employee involvement. Interview questions used for this segment can be found in Appendix A.

Mid-level Managers at Hanford

The primary focus of our research was on this particular segment. Mid-level managers are responsible for relaying information regarding the Security Education and Awareness Program (SEAP) to their employees, and for engendering personal commitment to its effectiveness. Therefore, it was important to identify their beliefs regarding the SEAP and any ideas that, if implemented, could enhance their ability to relay the information to, and encourage participation from, their employees. Interview questions used for this segment are located in Appendix A.

Primary Research

The bulk of our research involved conducting in-depth interviews with individuals in the segments described above. A total of 37 interviews were conducted both face-to-face and over the telephone as time and circumstances permitted. Interviews were conducted in an open-ended format, allowing interviewees to answer questions in a way they felt best conveyed their beliefs.

We also included aided and unaided recall questions in the interviews, to help identify successful communication tools. Aided recall involves recognition of an item when prompted either visually or verbally. Unaided recall involves retrieving information from

a person's long-term memory without prompting. Items that are recalled without a verbal prompt may be considered more effective in terms of gaining customer loyalty (Minor and Mowen, p. 58).

Alison Marcum and Sophia Orozco were given the opportunity to travel to Washington, D.C. to attend the annual Security Education Special Interest Group conference, held in Arlington, Virginia from April 9-11. Travel, as well as some of the funding was arranged for and provided by Washington State University. Chester Braswell provided substantial funding for this trip as well, due to the opportunity to increase the scope of the study. In addition to conducting face-to-face interviews, extensive notes were taken during presentations at the conference, as well as an analysis of promotional materials and ideas being implemented at other sites around the country. Samples of some of these materials can be found in Appendix B.

Secondary Research

A wealth of relevant information was also obtained electronically, via Washington State University's library database system. Many of these items will be discussed in later sections of the report, and are available in full text in Appendix C.

Competitor

Purpose

The purpose of this section is to analyze the competitive environment in order to identify potential opportunities for Protection Technology Hanford to increase security awareness and ownership at Hanford. Interviews with managers at Hanford and throughout the Department of Energy (DOE) conducted during this study indicated a strong recognition for the need to achieve personal commitment in order to achieve the desired levels of security awareness. This competitive analysis focuses on a comparison of security awareness programs with safety and health protection programs (safety awareness). There are similarities between these two protection programs, but interviews show that managers at Hanford recognize that the two programs are competing for priority as well as awareness. The Voluntary Protection Program (VPP), Integrated Safety Management (ISM) and Enhanced Work Planning (EWP) have all been successful at increasing awareness, perceived value, and safety performance at Hanford and other DOE sites over the past few years. This analysis identifies some differences between these competing programs that may help Protection Technology Hanford realize its vision for high levels of security awareness, commitment, and performance at the Hanford site.

Sources of Competition

Generally, the analysis of the competitive environment includes identifying those organizations that are competing for the prospective business of a particular group, or segment, of customers. However, for the Security Education and Awareness Program (SEAP) at Hanford, it seems to be more appropriate to consider the competitive environment in terms of competition for the employees' attention and priority rather than their business or specifically in terms of dollars alone.

Figure 5.1 depicts three levels of the competitive environment. The inner circle shows the security awareness program's direct competitors. This circle is entitled "Protection Programs" because each of the programs indicated are designed to protect against potential events that have undesirable consequences.

The protection programs for each of the Hanford contractors contribute to "Company Performance," the second circle. In this level of the model, the protection programs compete for manager attention and priority against other company performance needs. Managers must balance resources to achieve optimal performance across many elements such as production, budget, schedule, funding, and customer satisfaction. Managers place high value on achieving ownership of principles and values that support high levels of performance for each of these elements. These values are an integral part of national and international industry standards such as the Malcolm Baldrige Award, ISO 9000, ISO 14000, Integrated Safety Management (ISM), the Volunteer Protection Program (VPP), and the As Low as Reasonably Achievable (ALARA) concept for radiation protection programs. Each of these emphasizes performance-based standards rather than compliance.

The outermost circle represents the competition that occurs between PHMC companies vying for priority and funding to meet Project Hanford objectives; at the Project Hanford level, Protection Technology Hanford (PTH) competes with other site programs for these things. The services they provide must have sufficient perceived value in order for PTH to succeed as a Project Hanford contractor. In order to be successful in this outer circle, PTH must be able to influence its customers' perceptions as to the value of conducting work in a manner that protects security of the worker, special nuclear material, equipment, and information. Protection Technology Hanford's goal is to move security performance to higher levels by achieving greater worker commitment.

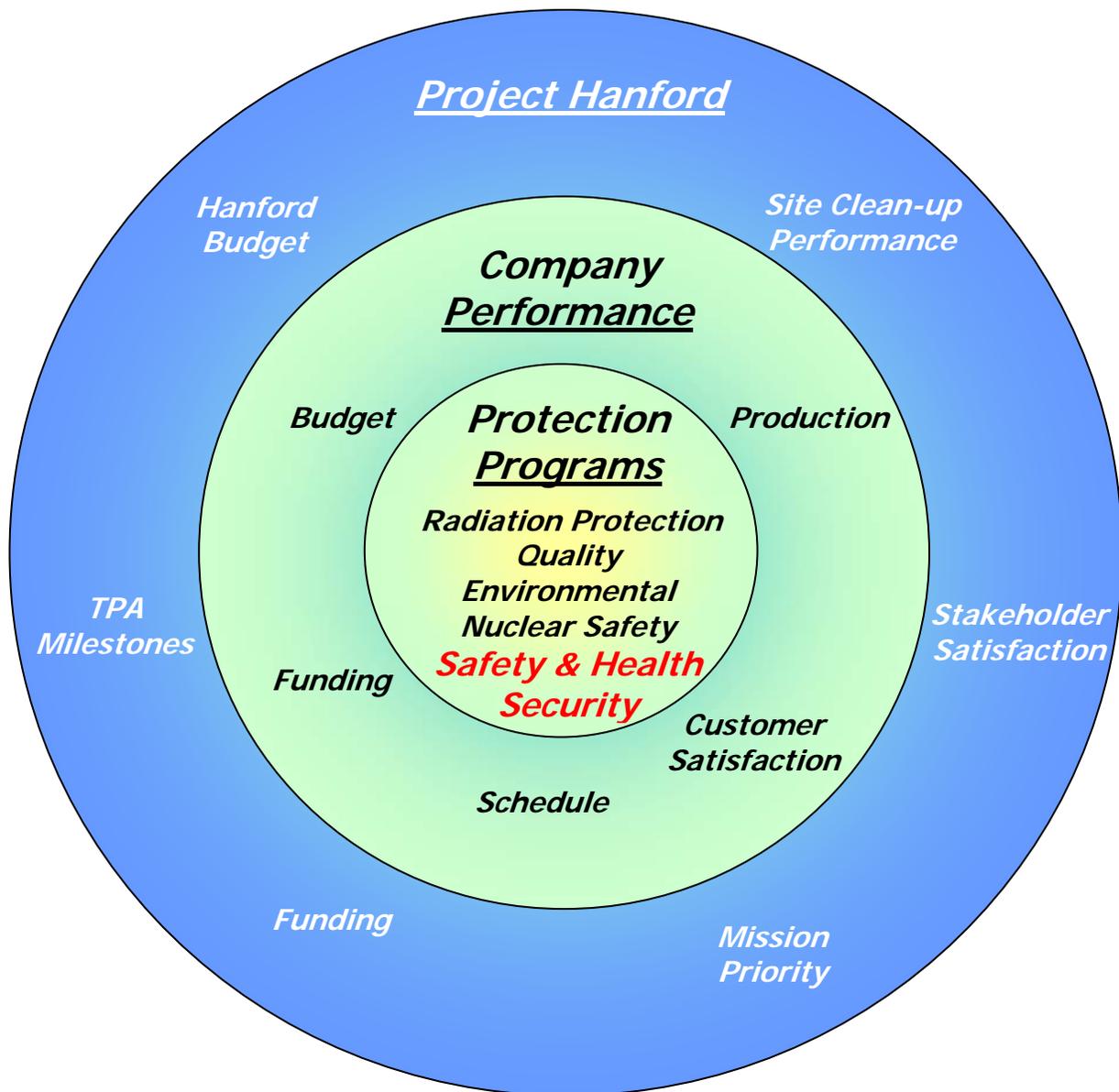


Figure 5.1 The Competitive Environment at Hanford

Case Study

Purpose

The purpose of presenting this case study is to note similarities and analyze some important differences between two protection management processes that seek to build ownership and encourage involvement. This case study supports Protection Technology Hanford's (PTH's) goal of improving ownership of the Hanford Security Education and Awareness Program. The DOE safety program, VPP, which is the security awareness program's primary competitor, has been chosen for this comparison.

Appendix C contains an historic comparison and analysis of DOE security awareness and safety programs, prepared as part of the case study. The information highlights the approaches and changes in security awareness and safety programs from the late 1980's to the present. This historic perspective provides not only a foundation for understanding, but also some insights into how implementation approaches have influenced the competitive position of the current security awareness program at Hanford.

How Safety Can Help Security

1) Similar functional goals

The security awareness programs rely on effective communication processes, well trained, dedicated, and involved workers to help recognize, eliminate and control workplace security threats (Habiger, March 2000, Appendix C). Similarly, the DOE-VPP relies on effective processes, well trained, dedicated, and involved workers to help recognize, eliminate, and control workplace hazards. The VPP program has established high standards of performance. DOE/VPP program managers provide assistance to improve safety processes and to develop workplace safety culture. (OSHA, 1989, Appendix C).

2) Compliance vs. Performance and Behavioral Approach

In the late 1980's and early 1990's DOE safety programs were unsuccessful at attaining compliance with safety requirements. In the mid-1990's, much expense and repeated failures occurred following a compliance-driven model for safety implementation at DOE sites. These failures resulted in loss of award fees and contracts in some cases. As a result, DOE made changes to a more effective approach that used safety performance rather than safety compliance as the standard. This approach was developed in the Occupational Safety and Health Administration (OSHA) and is called the Voluntary Protection Program (VPP). VPP changed the approach from one of trying to force compliance with safety to a new safety performance based approach that sought to change the safety culture. (Hanford VPP homepage; Total Safety Culture, INEEL homepage; Hanford Progress; Environmental Safety & Health, Safety Notes 1994, Appendix C).

The security awareness program faces challenges that are similar to those faced by safety programs in the mid-1990s when safety performance improvements were needed. (Analysis, Appendix C). The security awareness program has been based on a compliance standard but appears to be undergoing a change toward a performance-based approach. This desire to change was discussed during the initial study meeting. PTH Security Awareness Coordinator, Chester Braswell, expressed a desire to increase security performance by creating a "vibrant security culture" in which individuals are committed to following security policies at Hanford (C. Braswell, Personal Communication, January 2001).

3) Compatibility of Values and Beliefs

Interviews with security managers at Hanford and DOE Headquarters identified similar widely held beliefs and values. A composite performance indicator was created from these interviews. This indicator identified five characteristics of an outstanding security culture. The characteristics are ownership, management support, delivering the message, teamwork and security performance. (A.3; A.4; A.5; A.6; A.7, Personal Communications, March 2001). The VPP program is based on five tenets that are similar to characteristics identified by the security experts. The VPP tenets are: management commitment, employee involvement, worksite analysis, hazard prevention and control, and safety and health training. A brief description of each of these tenets is provided in (Hanford VPP Homepage, Appendix C)

These VPP tenets are understood and are part of the PTH corporate culture. The DOE-VPP Onsite Review Report that documented PTH's attainment of VPP Star-Status stated, "PTH has established such a strong safety culture that both management and employees share the belief that all employees of PTH are both responsible and accountable for **S&H** [safety and health] in the workplace" (DOE/EH-0645, 2000, Appendix C).

The values and beliefs that have strengthened the safety culture at PTH are the same values and beliefs identified as being needed to enhance the Hanford security culture.

4) Protection Technology Hanford and VPP-Star Status

Another important consideration for using VPP is that Protection Technology Hanford was one of the first ten contractors within the DOE complex to achieve VPP-Star Status (Reach, 2001, Appendix C). Protection Technology Hanford has successfully applied the concepts and principles of VPP within their own company as validated by independent experts (DOE/EH-0645, Appendix C). PTH's ability to involve employees and managers and gain commitment to safety was noted in the VPP Survey for Calendar Year 1999. The survey report recognized the outstanding safety performance of PTH employees in the following observation:

"The ongoing efforts of PTH employees in the safety council process has been the greatest asset of the Safeguards and Security program. Employees have true ownership of the programs and take steps to make the workplace and the work safer

for everyone. The PTH safety council process should serve as a model for others to emulate." (VPP Survey Results, 1999, Appendix C)

PTH has experienced success in its own implementation of safety programs through the VPP approach. A comparison of VPP principles and approaches to those of the security awareness programs can identify opportunities to apply what has been learned in VPP to achieve even higher levels of ownership for security at Hanford.

5) The VPP Approach Works

"It [VPP] is about working in partnership with common goals, instead of as adversaries, to protect the safety and health of our workers. It's about focusing a lot less on red tape, and a lot more on results. The Voluntary Protection Program is the premier example of partnership between government, management and labor." - Vice President Gore, 1995 (DOE/EH-0591, 1999, Appendix C)

A compelling reason to compare security awareness programs to VPP is because VPP has been exceptionally effective at accomplishing its safety goals at Hanford. One of the measures used by the Occupational Safety and Health Administration (OSHA) is the "lost work day case incident rate." This measure is determined by dividing the number of accident cases in which an individual misses at least one day of work, by 200,000. The number of hours in 100 years of work (OSHA, 1989, Appendix C). Hanford's "lost work day case incident rate" dropped 65% between October 1996 and October 2000, from 1.85 to 0.64 (PHMC, 1999; 2001, Appendix C).

Some Limitations in the use of VPP

While VPP is an excellent program with which to compare the security awareness program, there are some differences that pose a potential challenge. It is difficult for individuals to separate security awareness from other security program functions. Security programs rely on secrecy as a tactic in providing protection to people, property, information, and safeguard materials. As a result, within the security awareness program there are conflicting objectives between employee involvement and the need for secrecy. (DOE-RL Mgr 1, Personal Communication, March 2001) The resolution of this conflict defines the limitations of communication that can occur.

A second potential problem is how security personnel serve their enforcement function. The Hanford Patrol are here to deal with situations that potentially constitute a threat to the security of people, property, information, or safeguard material at Hanford. Their actions and behaviors in carrying out this function can send a confusing message. The security awareness program is seeking to reduce the barriers that separate it from the workforce. At the same time the workforce perceives that Hanford Patrol members are intentionally trying to maintain a separation from the rest of the workforce. This perception does not support the security awareness program's role of communicator, educator, promoter and facilitator. One Hanford worker described this situation very well in response to the email survey, conducted by the WSU-Vancouver research team.

"The work environment here on site (200E) is clearly different than any I have encountered in my career. Security consciousness is very high. I must say I find the Hanford Patrol to be very intimidating (black shirts, camouflage pants, dark sunglasses, high powered weapons in sight). I recognize this serves a purpose when it comes to ensuring security of classified information or special nuclear materials. However, it does make for a more difficult work environment. I would suggest that, since I am primarily responsible for security in my area of work, patrol officers could be perceived as supportive instead of threatening - at least in the site areas where no classified material or information is stored. Let's face it, in Tank Farms, we're just the mop and pail brigade cleaning up a mess." (Vancouver Report, 2001, Hanford Survey Data)

Security and VPP, Yesterday and Today

The security awareness program at Hanford is faced with a situation that is very similar to that of safety programs at the beginning of the 1990s. In a reversal of fortunes, safety has received a high priority and has been drastically changed over the past six years while the security awareness program has received less emphasis and support (C. Braswell, Personal Communication, January 2001).

The need to improve security awareness and performance became a high priority within DOE due to a series of high profile security incidents. These incidents raised serious questions and concerns in Congress. To help increase priority and security visibility, DOE created the National Nuclear Security Administration (NNSA), and indicated that security as well as security awareness programs, must improve. Today, DOE is expected to make significant improvements to security awareness, and more importantly, security performance. DOE is meeting this challenge by increasing emphasis and accountability for security performance. Senior DOE managers have recognized the need to change the culture of DOE so that security is once again an integral part of the way people think and do work (Habiger, 2000, Appendix C). Security awareness programs will most likely be called upon to help create this new culture.

The heightened level of concern about security is very much like the situation DOE was in with respect to its safety programs in the early 1990s. The initial approach by DOE was to direct contractors to comply with safety. An enforcement approach was used that included "Tiger Teams" comprised of safety experts that conducted compliance assessments of contractor safety programs. During this timeframe, DOE provided additional funds and implemented contract performance incentives for improving safety accountability. Despite increased funding, management involvement, and accountability at a corporate level, performance did not improve. Companies lost award fees as well as their DOE contracts for failure to engage the workforce. Neither DOE nor its contractors were being successful. It was recognized that there was a need to find a more effective way to achieve safety performance goals. DOE responded to this situation by adopting and implementing VPP. (Appendix C)

The expectations for the security awareness program appear to be changing. The program is attempting to make a transition away from a traditional compliance based protection program model, which relied on subject matter experts to create, cajole, and assess performance to standards. The result of this approach was that requirements were complied with but often not understood or fully accepted by the workforce. The new approach seeks to increase performance and ownership rather than settling for compliant behavior.

Communications

In the 1980s the security awareness and safety programs used similar approaches in communicating to, not with, the workforce. Both security awareness and VPP programs have continued to develop more innovative ways to communicate their messages. Both programs rely to some degree on subject matter experts to visit with work groups and provide technical support as well as encouragement to the workforce efforts to be effective.

In the late 1980s and early 1990's security was successful in using a traditional "telling" style of management because laws, DOE orders, and senior management supported the need for security. But during that same timeframe, when safety managers attempted to increase performance through positive and negative cash incentives and high visibility, but ineffective traditional approaches, they were unsuccessful at changing behaviors. When DOE adopted the VPP approach it changed both the way it communicated with workers and the kinds of safety messages it used (Tables, Appendix C).

Valuing approach

An element of the VPP approach that has not been used by security awareness programs is one of sending a consistent message that values individuals and draws on employees' experiences in a cooperative sharing process. (Total Safety Culture, INEEL, Appendix C) This VPP approach engages individuals on an adult-to-adult basis that increases efficiency and productivity of the workforce. (VPP Survey Results, 1999, Appendix C)

Worker-to-Worker Communication

An important difference between the security awareness program communications and VPP is the maturity and use of employee communications networks. While there are few networks being effectively used to convey information or work on security issues, the VPP approach has actively promoted worker involvement in developing and communicating its safety messages. Employees that participate in VPP help to develop formal safety messages and identify situations and lessons learned information to be communicated to the workforce. Individuals that prepare safety communications and those that act as representatives for their own workgroups are part of the VPP communication process and infrastructure. (Total Safety Culture, INEEL, Appendix C)

Workers are the Medium

These VPP networks of communicators are a medium that is being used to communicate safety awareness and to influence safety behaviors. This "word-of-mouth" communication medium is an integral and vital part of VPP. In his book, "The Medium is the Message," Marshall McLuhan notes that the medium carries its own message. For example, television's is primarily an entertaining medium and its message is entertainment. McLuhan asserts that the medium that carries the message influences how the message is interpreted and that the message influences the medium is perceived (M. McLuhan, 1965). The VPP communications networks of individual workers are comprised of interpersonal contacts. Each interaction includes exchanges of information with emotional content. In their textbook on consumer behavior, Minor and Mowen, analyze word-of-mouth communication. They point out that word-of-mouth communication fulfills the needs of the senders to influence others. The exchange of information increases the sender's influence, which in turn increases the sender's confidence in their decision to "buy the product." This process can also potentially increase the sender's involvement within the group. Increased involvement and respect from the group reinforces by building the individual's feelings of power and prestige. (Minor & Mowen, 2001). The VPP approach makes use of these benefits that are derived from interpersonal relations.

The word-of-mouth message is an important contributor to VPP success. Using employees to create and communicate the safety message has made the message more relevant while at the same time building acceptance and reinforcing ownership of the importance of safety. Workers like to share their safety experiences with each other. The formal and informal messages they communicate are their own; the process helps to both express and develop their commitment. Through these interpersonal relations they convey emotional messages of commitment and mutual support that are well received by the workforce (Vancouver Report, 2001, Hanford Survey Data).

Expert-to-Worker vs. Worker-to-Worker

The traditional compliance approach for implementing protection programs, including security, was based on an expert-to-worker (parent-to-child) relationship. In interviews, the security awareness coordinators and managers across the DOE complex demonstrated that they understand the need to improve relationships between security awareness and employees (Industry interviews, Personal Communication, March 2001, Appendix A). However, an analysis of the content of security messages indicates that some expert-to-worker messages are used. This appears to be a communication skills issue because of the expressed desire of the security awareness professionals to team with employees. The communication patterns that were successfully used to implement a compliance approach are incompatible with worker involvement strategies.

This conflict between the cognitive message and emotional message is interpreted as being an incongruent dual message. Sending dual messages can confuse the meaning of the message and reduce communication effectiveness. An example of this type of incongruent message appears in the Vice President Gore's statement as previously quoted.

"It [VPP] is about working in partnership with common goals, instead of as adversaries, to protect the safety and health of our workers. It's about focusing a lot less on red tape, and a lot more on results. The Voluntary Protection Program is the premier example of partnership between government, management and labor." - Vice President Gore, 1995 (DOE/EH-0591, 1999, Appendix C)

The use of "our workers" in this statement can be interpreted to imply a protective, parent-to-child relationship, which is "our workers are like our children." This thought is not congruent with the concept of "partnership" described two sentences later.

It is not a question of what the Vice President intended to convey. The communications issue is does the message get received. Fortunately, communication relies on more than words. It is doubtful that anyone participating in the meeting with the Vice President questioned his endorsement of VPP, as his presence and actions demonstrate his management commitment. But, what would the message have been if it had been read by an assistant, to an aid, to the Vice President? This highlights the value to be gained by direct contact between managers and workers. Management actions are another medium that helps to clearly communicate and reinforce managers' attitudes, beliefs, values and expectations.

Employee and Manager Involvement

The level of employee and manager involvement is a major difference between the two approaches. Safety and Health programs have achieved significant changes in attitudes, beliefs, values, behaviors and performance over the past several years (DOE/EH-0591, 1999, Appendix C). Although security awareness program coordinators value individuals, they are not using and empowering employees and managers to develop and help deploy those aspects of security that directly impact their work environment. Instead, security awareness programs rely on security subject matter experts to perform these functions. This program approach does not encourage management commitment or employee involvement, thus reduces levels of ownership for security. (Industry interviews, Personal Communication, March 2001, Appendix A).

The need to maintain appropriate secrecy in some activities is an important element of security awareness that does not affect the VPP program. Secrecy issues have hampered efforts to clearly communicate the consequences and frequency of security lessons learned. This conflicts with the need to communicate DOE or industry experience to the general workforce, which puts the Security Awareness program at a competitive disadvantage with VPP. (DOE-RL Mgr 1, Personal Communication, March 2001)

The VPP program differs from the security awareness program in the level of direct involvement of employees. DOE-VPP program managers, during a preliminary review of Savannah River for VPP-Star Status, raised concerns about the traditional, "one size fits all" approach being used at that time. This that approach leaves workers powerless to take any initiative. The report concluded that in that situation the workers become reliant

on managers or subject matter experts to mitigate issues. (DOE/EH-0591, 1999, Appendix C).

When a similar review of PTH was conducted in August 2000, it found that; employees of PTH are involved in the promoting of safety in their workplaces. In many ways PTH has both a Safety Council and a Patrol Safety Council that act as forums for workers involvement. Workers prepare job hazard identification, analyses and resolution tasks; they also conduct self-assessments and safety walk-around activities. The report extolled the evidence of inclusion of individuals in the language used. They referred to their efforts using terms like “we” and “our”. (DOE/EH-0645, Appendix C) According to the PTH Security Awareness Coordinator, the Hanford Security Council is comprised of security professionals from Hanford and does not include employee representatives. This inclusive and interpersonal teaming contributes to VPP's success as a program and as a competitor.

Performance Measurement

The VPP program at Hanford uses fifteen elements in a survey format to evaluate performance. The following list contains sample measures from each of the five areas being monitored. The statements use a scale that ranges from "Strongly Disagree" to "Strongly Agree."

- 1) Senior management visits your workplace;
- 2) You are involved in decisions affecting your safety and health;
- 3) Responses to your reports of hazards are timely and adequate,
- 4) You have seen safe work procedures fairly and consistently enforced; and
- 5) The safety and health training you received is appropriate for your job.

The survey results, which provide the baseline for VPP performance, show a high level of agreement that the tenets of VPP are being implemented at Hanford. VPP is using a statistical process control approach that measures behaviors but does not measure attitudes or beliefs (VPP Survey Results, 1999, Appendix C).

No published measures of security awareness at Hanford were found on the Hanford web pages. Interviews with security awareness coordinators and managers across the DOE complex identified that no behavioral, attitude, or belief based measures being used. The only measures of security awareness mentioned during the interviews were the results of quizzes, critiques of training and tracking the number and types of security infractions (Industry interviews, Personal Communication, March 2001 Appendix A). Tracking security infractions is equivalent to the "Lost Work Day Case Incident Rate" measure used in the safety program.

One of the goals of this study was to determine the current baseline of security awareness. The email survey that was conducted provides valuable information but does

not provide baseline information on the affective and behavioral elements of security awareness program effectiveness.

Summary

Security experts indicate that the security function is still perceived as a barrier by many DOE workers. However, recent actions indicate that security awareness is on the threshold of a change that has the potential of influencing the perceptions of its value. Safety and Health was once seen as a barrier to getting work done, but is now nearly fully integrated with the way people think about doing work, and is generally perceived to be helpful in getting the job done right.

It is appropriate to compare and consider the effectiveness and approach of VPP to security awareness. The safety program changes that were made in the mid-1990s have had a dramatic impact on safety at Hanford. Safety and Health performance at Hanford improved 65% between October 1996 and September 2000.

The following changes occurred in the safety programs when the VPP approach was adopted:

1. **Valuing Employees:** There was a change in how subject matter experts valued the employees. This changed views of the workforce. Workers are now viewed as customers and partners rather than subordinates and barriers to achieving safety goals.
2. **Treating everyone as an expert:** There was a change in the relationship between safety and its customers. The traditional expert-to-worker relationship was abandoned and a worker-to-worker approach was adopted.
3. **Leveraging influence through worker involvement:** The safety program began to involve employees in every aspect of development and delivery of the safety program. This involvement has led to higher levels of ownership.
4. **Using the "people channel":** Employee involvement created a new and powerful communication medium that has increased awareness, involvement, ownership and performance.
5. **Measuring performance:** Safety began to measure the behaviors that were needed to achieve desired performance in addition to lagging measures such as "lost work day case incident rates."

These five implementation strategies appear to separate the VPP approach from the current Security Awareness Program approach. The implementation sequence is as follows:

- VPP process started with DOE and Corporate management buy-in.
- Employee Involvement was then initiated
- This involvement improved communications, built cooperation and trust, and increased ownership and commitment.
- Employees conducted site and facility specific analysis, building their knowledge
- Employees helped identify expectations and processes to improve controls, monitoring, and accountability
- Training was reinforced through employee-to-employee communications
- Effective safety performance was achieved

Table 5.1 shows there are similar beliefs held by VPP managers, the Security Awareness managers at Hanford, the Security Awareness managers that participate in the Security Education - Special Interest Group (SE-SIG), and security and other experts published in the literature. However, implementation between the two varies. The VPP implementation provides the standard for achieving involvement, cultural change, and improved performance. Areas shown in blue on the table identify where the Security Awareness Program is implementing practices that do not appear to be supportive of the program's goals. The table identifies resource articles that support achieving higher levels of worker involvement and implementation of successful security awareness strategies. Many of these articles can be found in their full text versions in Appendix C.

Opportunities for Security Awareness To Benefit from VPP Strategies				
VPP		Security Awareness		Security & Support Literature
Belief	Implementation	Belief	Implementation	Helpful References
Management Commitment	<ul style="list-style-type: none"> Safety is a management priority 	Management Support	<ul style="list-style-type: none"> Security Awareness is a management priority 	(References 1, 2, 3, 4, 21) Increasing management support
	<ul style="list-style-type: none"> Line manager "walkabout" 		<ul style="list-style-type: none"> Security manager "walkabout" 	
	<ul style="list-style-type: none"> Managers sponsor workers' efforts 		<ul style="list-style-type: none"> Security lack sponsorship in 1990's, & had resource limitations 	
Employee Involvement	<ul style="list-style-type: none"> Safety teams & committees have open two-way communications 	Employee Ownership	<ul style="list-style-type: none"> Teaming with workers is not done 	(References 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 21) Building liaisons with other organizations. Team building, employee involvement actions
	<ul style="list-style-type: none"> Safety communicates <u>with and through</u> the employees 		<ul style="list-style-type: none"> Security communicates <u>to</u> employees but not <u>with and through</u> them 	
	<ul style="list-style-type: none"> Employees drive programs 		<ul style="list-style-type: none"> Employees do not generally help develop security awareness 	
Worksite Analysis	<ul style="list-style-type: none"> One size doesn't fit all 	Security Conscious Workers	<ul style="list-style-type: none"> One size fits all, mass media approach 	(References 15, 21) Using inputs from employees to build acceptance of security measures
	<ul style="list-style-type: none"> Workers analyze using subject matter expert as a resource 		<ul style="list-style-type: none"> Subject matter experts conduct security reviews without worker involvement 	
	<ul style="list-style-type: none"> Employees monitor and participate 		<ul style="list-style-type: none"> Workers reluctant to identify potential security issues in their work locations 	
Hazard Prevention & Control	<ul style="list-style-type: none"> Workers develop and choose controls 	Worksite Surveillance	<ul style="list-style-type: none"> Security determines controls without explanation 	(References 15, 21) Using inputs from employees to build acceptance of security measures
	<ul style="list-style-type: none"> Effective controls are in place 		<ul style="list-style-type: none"> Badges and physical security measures are in place 	
	<ul style="list-style-type: none"> Workers hold themselves and each other accountable 		<ul style="list-style-type: none"> Worker hides badge in defiance of security in a "make me" behavior. 	
Safety & Health Training	<ul style="list-style-type: none"> Employees and subject matter experts lead small group discussions 	Training	<ul style="list-style-type: none"> Employees do not lead training, HGET, mass media, posters, video 	(References 3, 16, 17, 18, 19, 20, 21) Training resources, messages, and approaches
	<ul style="list-style-type: none"> Managers involved in training 		<ul style="list-style-type: none"> Some managers make presentations and are involved 	

List of Table 1 References.

Note: Copyright protection has prevented the inclusion of some these documents in the appendices of this study.

1. Security's Positive Return; Security Management; Arlington; January 2001; S. Harowitz
2. Behavior-Based Accident Prevention Program (BBAP); LBNL; July 1999; J. Chung, Internet,
3. How to build a comprehensive security awareness program; Computer Security Journal; San Francisco; Spring 2000; Tom Peltier
4. Getting executive attention; Security Management; Arlington; January 2000; MacDonnell Ulsch
5. Staff the suggestions box; Total Quality Management; Abingdon; August 1999; Geoffrey Lloyd
6. Whose mission is it, anyway?; Security Management; Arlington; April 2000; S. Kandiah, Y. Kiong
7. Cultivating commitment; Association Management; Washington; March 2001; P. DePas
8. Merger, they wrote; Security Management; Arlington; March 1999; Teresa Anderson
9. How teamwork can be developed as an individual skill; The Journal for Quality and Participation; Cincinnati; Fall 2000; Christopher M. Avery
10. Security motivation, the mother of all controls, must precede awareness; Computer Security Journal; San Francisco; Fall 1999; Donn B. Parker
11. Using ISO 9000 and ISO 14000 Together; ISO Homepage.
12. VPP implementation descriptions from INEEL; INEEL Homepage
13. Crafting a cohesive program; Security Management; Arlington; March 1999; Mark S. Lex
14. Weisbord, M. R. (1987). Productive Workplaces, Organizing and Managing for Dignity, Meaning, and Community. Jossey-Bass
15. An ounce of prevention; Building, Cedar Rapids; March 1999; Regina Raiford
16. Overcoming insecurity, Computerworld; Framingham; July 2000; Deborah Redclif
17. Companies aim to build security awareness; Computerworl; Framingham; November 2000; Dan Verton
18. Safety for hire; Business Mexico; Mexico City; August 1999; Tom Dieusaert
19. Corporate espionage can't be this easy; Security Management; Arlington; September 1999; E. G. Ross
20. Security awareness week at the Pentagon; Journal of Electronic Defense; Norwood; November 2000; Kernan Chaisson
21. VPP Best Practices Submittal Forms; DOE VPP Homepage

Concluding Analysis

The Security Awareness Program is striving to increase awareness, ownership and performance at Hanford. They have demonstrated their success at building awareness and meeting compliance requirements, but the task of building ownership is not easy. This competitive analysis shows how increasing worker and management involvement helped improve the safety culture at Hanford in the 1990s. To improve the security culture at Hanford, the challenge is to find an effective way to integrate worker and manager involvement into the security awareness program.

The safety programs have successfully changed the safety culture at Hanford and elsewhere by creating an environment that fosters a high degree of awareness and ownership. There are two major differences between the Safety and Health and Security Awareness programs: 1.) The level of management priority and accountability. 2.) The Safety and Health program has been extremely successful in building ownership through worker involvement.

The following are conclusions about how these changes have impacted the success of Safety and Health.

Management priority and accountability are important but are not enough.

There has been a high degree of emphasis placed on improving safety performance by DOE. Staffing and funding levels for safety programs were increased in the 1990s, including substantial inducements in contract award fees based on safety performance. The prime contractors made commitments to achieve improved safety performance, and the increased funding levels allowed management to increase emphasis. However, initial attempts were not successful in changing the safety culture. DOE and these companies learned that changes to the safety culture could not be instantly achieved. Nor could they be directed or created through inspections.

In the early 1990s, management increased safety visibility by applying increased resources, and by becoming more involved and providing clear direction about their safety expectations. This approach was similar to that used in the 1980s to successfully achieve security compliance at DOE sites, however the workforce resisted this direction and behaviors didn't change. Increasing resources and gaining management commitment were not enough to improve safety awareness and performance. Prime contractors at several DOE sites (Hanford, Idaho, Rocky Flats, Oak Ridge, and Brookhaven) were unsuccessful at achieving improved performance despite increased funding, priority, accountability and management direction. A cultural change was needed to achieve desired safety performance behaviors.

Worker involvement must accompany management commitment:

The adoption of OSHA's Voluntary Protection Program (VPP) by DOE caused safety managers to change their entire approach toward building awareness. The program focused on rebuilding safety from the worker up. It involved workers and managers from diverse parts the organization who participated in improving the delivery of safety programs and the safety message to the workforce. The Subject Matter Experts (SMEs) became facilitators that helped the workforce build effective safety programs while building ownership and consensus. The facilitating role of the SMEs changed the workforce's perception about them from being the "safety police" to being the "safety resource." Perceptions of the value of safety professions increased as ownership for safety passed from the SMEs to the workforce. Safety performance increased as the level of ownership improved.

Industry

Overview

Security is a critical part of conducting work at the Department of Energy (DOE). A key element of the security program at Hanford and other nuclear sites in the U.S. is protecting information or materials that could be used to endanger national security. However, employee attitudes and perceptions at the sites were influenced by the end of the cold war and by a transition in the DOE mission. Where they were once conducting highly classified and secure work that supported national defense, they are now primarily involved in the cleanup of an environmental super-fund site.

At cleanup sites, building and maintaining security awareness and ownership is an important goal. Delivering quality training, providing effective security awareness activities, and increasing management ownership are viewed as key contributors to building and maintaining workforce acceptance and responsibility for security. All governmental sites have security programs. However, not all sites use the same training and education material or techniques to achieve security awareness and performance.

Security awareness program managers and coordinators from Pantex, Idaho National Environmental Engineering Laboratory (INEEL), the Oak Ridge National Laboratory (ORNL), and National Nuclear Security Administration (NNSA) Oakland Operations Office, and Albuquerque (FMNT) were contacted and asked to describe their programs and identify elements that they believed to be most and least effective. In addition to security awareness managers, several interviews were conducted at the SE-SIG Conference in Washington D.C. The following discussion captures the self-identified "best practices" from these security managers and identifies specific activities being used to train as well as to help increase employee participation and ownership in DOE security programs.

There are many factors that contribute to the successful implementation of security programs. An activity that is effective in one organization may not be effective in another. Many activities identified in this section may be appropriate and easily implemented at Hanford, while others may not apply. However, they serve as a catalyst for reaching the next generation of great ideas.

Most Effective Practices

Interpersonal Communication – Face-to-Face Interaction

Person-to-person training has been very effective in gaining responsibility and ownership among employees at government sites across the country. This kind of training could be done through the initial training process as well as meetings and updates by supervisors. This type of training personalizes and gives a human aspect to the security program. With these types of feelings evoked in their workforce, employees are much more likely to be involved in helping the program succeed.

The training at Albuquerque is tailored to be meaningful to the workforce. New employee training is always done face-to-face. The first contact with security is made in their initial training, where new employees are paired up with a security professional that is also a trainer. The trainer takes the employee on their first tour of the facility; introducing them to others, and helps them become oriented with the facility. Albuquerque selects only those who are naturally friendly and have good interpersonal skills as trainers. The security coordinator at the Albuquerque site emphasized that a significant benefit of this approach is that the trainers are positive role models and representatives of the site security force. They form an initial bond at the facility with these new employees, which helps personalize security and increases the new employees' awareness and ownership from day one. "It is a good thing for them to bond with security. The other day a new employee made a point to wave to me."

(A.6, Personal Communication, March 2001)

"We are a small group. We have excellent relationships. We do give-a-ways, we use a customer service model, and one of the security people gives the tour of the compound and turns the worker over to the supervisor. This is a bonding process. They wave to us because they have bonded with us. Our approach is "person-to-person." We [security] are participating in all of the morale building activities, charitable functions, and employee teams so that we are part of the culture. It's not "us and them" here. We have picked the right people to present the initial training. We are delivering security like total quality, ISO 9000, and Integrated Safety Management. It's easier and better being accepted and liked." (A.6, Personal Communication, March 2001)

At Pantex the initial security awareness briefing is delivered face-to-face by security, but only hits the highlights of the security topics. The Actual training occurs in the workplace. Workers receive support from their supervisors and security subject matter experts. (A.9, Personal Communication, March 2001)

The record of low instances of security infractions at Pantex is attributed mainly to dedicated face-to-face supervisor-employee communication. When managers take the time to discuss security issues, employees take it much more seriously and are more likely to have a greater sense of ownership due to the human element it adds. (A.9, Personal Communication, March 2001)

Pantex security managers try to spend at least four hours per day out in the field. "It is important that the workers know us. We are working cooperatively to help people be successful." (A.9, Personal Communication, March 2001)

At Oakland Operations Office the security awareness team tries to see everyone at least once each year, "so they will know that security is not just a program. I am working to help them. My most important message is that we must work together to make security work." (A.10, Personal Communication, March 2001)

Guest Speakers

The use of guest speakers helps bring excitement and liven up what could potentially be viewed as dry subject. Guest speakers are able to entertain while providing useful information about a security topic and allow important security messages to remain fresh in employees' minds.

INEEL and Albuquerque maintain awareness by periodically bringing in guest speakers that provide "fun and interesting" security presentations that help to keep security issues of importance fresh in the employees' minds. Albuquerque does not generally require attendance at these meetings. (A.11, A.8, Personal Communication, March 2001)

Logo/Slogan

INEEL has experienced success with its logo and slogan contest. All ideas come from the workforce, as security group members are not permitted to submit ideas to the contest. Hundreds of ideas from the workforce are submitted for review, thereby creating a more involved workforce. INEEL indicates that its computer-based training has also helped expand awareness and foster ownership among its employees. It allows employees to refresh their own awareness and participate at their convenience.

At INEEL, the security trainer reported some unique and effective ways that security there has been improved. INEEL participates in an annual security contest to develop a new logo and slogan for security. Prizes are awarded for the logo and slogan that best demonstrates why security is important and should be taken seriously. The winning logo and slogan are placed on calendars and passed out to the workforce to help maintain security awareness and ownership. (A.11, Personal Communication, March 2001)

Demonstrations

The use of demonstrations allows workers to physically interact and discuss important issues. Employees are much more likely to take ownership if they can actually see the results of the practices currently in practice.

"We are doing a summer project this year that is exciting. There will be an office cubicle with all types of security discrepancies. People will be able to walk into the cubicle. One of the facilities at INEEL did this and had great success. The security discrepancy cubicle exhibit has been wonderfully received. It gives people a chance to see, physically interact, and discuss the security discrepancies they see in the cubicle. I have overheard people in the lunchroom discussing what they saw. This is fun way for people to learn. It's more hands on." (A11, Personal Communication, March 2001)

Surveys

Albuquerque conducts surveys on a periodic basis. " We found that people wanted to see the results of the survey. Now we tell what actions are being taken. We think this will increase willingness to participate because they will see how their inputs are used to improve the program. Much of the workforce is curious about the results of these

surveys and wants to know what is being done in response to these surveys. Sharing with employees the results of the surveys and actions taken increases the willingness of employees to participate in such studies because their input is actually used to help improve the program." (A.8, Personal Communication, March 2001)

Security Hotline

Pantex has established a hotline that allows employees to make anonymous contact with security. "We need to help people identify potential security problems. People are often afraid to tell about concerns they may have. Some people don't want to get involved or worry about being hurt by making contact. Some are afraid they won't be liked." (A.12, Personal Communication, March 2001)

Personalized Feedback

Albuquerque uses testing and training evaluation feedback to verify the effectiveness of their that their program. When an employee answers incorrectly a test question, the manager contacts the employee to help answer questions and to make sure they understand the security issue and why it is important. This is a non-punitive, supportive contact. (A.8, Personal Communication, March 2001)

Least Effective Practices

Mass Media

Most DOE sites implement marketing strategies that incorporate the use of mass media, which include such things as posters, signs, and bulletin boards. This type of media communicates the same message to the entire site, not taking into consideration the mission or special circumstances that each site operates under. The use of mass media sends a message of "one-size fits all", however research results have shown that one size does not fit all due to the variety of missions through out the DOE complexes. The "one-size fits all" approach communicates a message that all DOE sites are the same, when in fact they are all very different. When an employee is repeatedly given security material that does not apply to their job functions in any way, they are much more likely to overlook relevant security information when presented to them.

Read and Sign

Read and sign is one of the most commonly used forms of mass media used across DOE sites today. However the drawbacks to read and sign may outweigh the advantages. Read and sign can easily be ignored. The placing of read and sign can be ambiguous at best, and the messages can be complicated and hard to comprehend. Another factor that makes read and sign ineffective is that employees are not likely to absorb what they see, unless they are extremely interested or captured by the Many security managers from across the country named this material as the number one least effective aid, due mainly to the fact that employees just don't seem to read before signing.

“I don’t think read and sign works well. It doesn’t get the message across. Interactions are needed to fully commit to doing the right thing.” (A.9, Personal Communication, March 2001)

“We don’t rely on read and sign. When people are willing to take time to come and talk about security, then it must be important.....If a person makes a mistake a read and sign protects the company, but when I can look them in the face there is more accountability.” (A.11, Personal Communication, March 2001)

Posters have a hard time keeping up with the constant change occurring at facilities. Many times, posters are hard to understand and contain hidden messages. There is too much information for employees to effectively absorb whatever message the posters are trying to get across. (B.1, Personal Communication, April 2001)

“We used to use posters, but they are of limited use because they are no longer noticed after a couple days. We need more innovative ways of sending the message.” (A.5, Personal Communication, March 2001)

Computer Based Training

Computer based training is very convenient to the workforce at DOE sites, because it allows employees to work on security training at their desk, or their own time. However there are some major drawbacks in attempting to gain commitment and ownership among workers when implementing such training as was seen across many DOE sites. There is currently not a way to measure how effective the material is in gaining ownership and compliance. There is also no established way to determine if employees understand the messages that are being expressed. Further more, there is no way to determine if the employee even reads or takes the training seriously.

“Technology can take away the personal element. This may be hurting security awareness at some of the programs.” (A.9, Personal Communication, March 2001)

“This year we used a CBT and used the ‘so you want to be a millionaire’ approach to provide the briefing.....The people got lost in the logic and the results showed that they didn’t pass the training. It was a good idea that wasn’t implemented well. As soon as we realized what was happening we let everyone know.” (A.9, Personal Communication, March 2001)

Expert Insight of Security Awareness Culture

A sample performance indicator that describes and evaluates DOE security awareness culture is included in Appendix A. The sample, "Security Awareness Culture" performance indicator was derived from the results of five structured interviews. These results are not valid because of the sample size, but they are helpful in defining Security Awareness success. The indicator also demonstrates a method to measure "fuzzy" concepts such as culture, ownership, involvement, or satisfaction. Appendix A provides a process for developing this type of measure. The following description of an outstanding security awareness culture is based on the interviews conducted to create the security culture performance indicator.

"A security awareness culture has ownership for security principles. Individuals value security and understand why security is important to them. Managers are actively involved in the delivering the security message. They demonstrate the importance of security through their actions, and have a clear communication path between themselves and their employees. Programs deliver effective and relevant messages that are easily understood, accepted and delivered by managers to the workforce. The performance of the program is routinely evaluated to ensure it is achieving its goals of awareness and ownership." (A.1-A.7, Personal Communications, March & April 2001)

Conclusions

As representatives of the industry, the DOE sites contacted are addressing many similar issues to improving workforce security awareness and ownership. It is evident that there is a high degree of ownership by security awareness coordinators and managers who are dedicating time, energy, and resources to maintain and build security awareness.

There appear to be no effective tools for measuring security ownership, an essential security awareness goal that was often referred to in the interviews. There is also no evidence of detailed evaluations being made of the value that various activities contribute to awareness and ownership in the workforce. As a result there is no sound basis for determining return on investment or activities identified or optimizing the security awareness messages.

Each site is solving similar problems independently. The use of networking in the industry is high but does not appear to involve joint problem solving for DOE-wide issues. The Security Education Special Interest Group appears to be an organization where crosscutting needs may be explored and new tools for developing security awareness program capabilities, and evaluating the effectiveness of their performance can be explored.

Customer

Understanding employees' security awareness and ownership required that we start analyzing at the managerial level. This would reveal how much of the security message is getting to the managers and in turn, being sent to employees under their supervision. By asking open-ended interview questions we were able to get a general feel for manager attitudes and their AIM:

Approach

Involvement (Ownership)

Media (Usage, Response, and Preference)

Approach

The approach aspect of managing security will be defined as what is communicated and how it is communicated. Not all managers promote or enforce security in the same way. Some managers are doing more than others and this can be attributed to the role they feel is appropriate. Following the cold war, many changed their role as well as their approach to emphasize security less.

Change of Mission

The first and most widely recognized indicator of lower security awareness and ownership is the message that security has become less important since Hanford changed its mission. A change in mission from production to clean up has resulted in a lower perception of the importance of security. Perceptions of the importance of security are directly related to the level of involvement; that is, the higher the perceived importance, the higher is the involvement.

When production was the focus, many employees required clearances; hence, there was a constant reminder of strict security and consequences for infractions. There was a prestige associated with having a security clearance. When cleanup began, there were fewer Hanford areas requiring high security and, as a result, many clearances were terminated. The removal of some clearances and not others created a "caste system and losing the clearance meant losing status." This manager also stated, "when security was taken away, it was like a slap in the face. Many employees began feeling mistrusted" (A.31, Personal Communication, March 2001). This change was difficult for some and losing their clearance left many employees feeling resentful and apathetic.

At this time there was also a reduction of the number of patrol officers. Observing this cutback sent a nonverbal message that security was only important in patrolled areas. Although our interviewees expressed some complaints about the guards, managers mentioned that they are definitely important, in fact they are a "necessary evil" (A.23, Personal Communication, March 2001). A large number of managers think there is a

direct relationship between awareness and compliance of their employees and the number of guards present. They even suggest that the addition of guards would improve awareness and ownership at the Hanford site.

When referencing the Plutonium Finishing Plant (PFP), interviewees saw no change in security. All other areas noted a decrease in security importance. This perceived unimportance might lead to a low-involvement employee, who will take little to no interest and put forth virtually no effort to meet security goals. It may not be necessary or efficient to increase the number of patrol officers; however, other measures should be taken to increase awareness. In some cases, interviewees noticed an increase in security in the last couple years. They attribute this increase to the nature of the work being done.

Frustrations/Problems

The majority of interviewees stated that they do not have any frustrations, nor have they had any frustrations expressed to them in regards to security. These responses came primarily from the employees in administrative (office) jobs. However, some frustrations were expressed in areas perceived to be highly secure areas. Security in these highly secure locations is considered more important and results in higher personal involvement. At these locations, security cannot be avoided; it is dealt with on a day-to-day basis. This constant security interaction results in increased opportunities for problems to arise and for employees to experience frustration with the system. Problems/frustrations include the difficulty in understanding security expectations or why certain policies are in place. Many procedures are thought to be subject to interpretation, making it difficult to fully comprehend. These issues frustrate employees, and leave them feeling victimized by security, not empowered by it. When working with higher involvement people it is important to know that they attend to information more, they think more about the processes or changes and they are involved enough to give the idea time and effort. Many high-involvement people also prefer to be given the option to participate in the development of policies and procedures (Minor & Mowen, p. 38-40).

Effectiveness and Participation

Overall there are positive feelings about security effectiveness. The most successful elements of the program are seen as audits, patrols, and reports. In the eyes of employees, these tools enforce the importance of security, making their efforts worthwhile. Although these militant tactics bring quick results, these results are only short term where intrinsic motivation is low (Mero, Rizzo & Tosi, 2000). The constant threat of punishment will not foster the genuine belief and support of security. One will not grow a sense of security integrity through these means.

Improvements in the security program that are on the managers' wish list are more specific rules and procedures. As far as gaining employee participation, managers stated that is best done through the safety program. The only aspect of the security program recognized by managers to accomplish employee participation, are the guest speakers whom often appear during scheduled meetings. Those who had the opportunity to sit in on a talk seemed to have enjoyed it and had only positive responses. The small group

environment allows for individual attention and makes a comfortable environment for people to ask questions and voice their opinions. Many employees still need to be informed on why security is important, what is being protected, and why certain procedures are necessary. This first stage of gathering information is best done in one-on-one situations (door-to-door sales). In this atmosphere the speaker can better assess if there is any miscommunication and see where information is lacking. From the responses it is obvious that employees can reiterate the rules and know the consequences, but do they go beyond that and know why? Will they try to follow and encourage others to follow guidelines as well? Are consequences for non-compliance enforced?

Tools

To foster outstanding security awareness there must be an understanding of responsibilities with real consequences. Consequences for the manager as well as the employee are recognized to range from a warning, to a poor performance rating, to suspension without pay, and finally termination. Of course these consequences are dependent on the nature and magnitude of the incident and are open for review. Some refer to the *Project Hanford Management Contractor (PHMC) Standards of Conduct* for guidelines to follow (A.32, PHMC Standards of Conduct). Unfortunately, many expressed that although they are aware of these consequences, they are frustrated because they are not consistently enforced. Ambiguity seems to exist as to who is responsible for the enforcement of consequences.

Using real incidents to communicate security's importance was a common suggested solution among interviewees to increase security awareness. These examples need only to be situationally relevant, not necessarily Hanford specific. Many employees do not hear of security breaches so they are not aware of any problem. The attitude of some, follows the adage, "why fix something that is not broken." Describing these incidents can increase the fear and respect for security; employees may begin to understand breaches can and do happen. As a result, you will have more involved employees. Another suggestion was to keep employees aware with continual reinforcements. "Get out there more and be repetitive" (A.30, Personal Communication, March 2001). If employees see security personnel believing in the cause enough to make appearances and preach its importance, they, too, may begin believing. Being present also makes security part of their everyday work. If done in a friendly manner, employees will also develop a positive, helpful image of security.

Involvement

A person's level of involvement can be related to their perceived importance of the idea. Managers most often view security importance as "very" or "extremely" important. One remark was that security is "only second to safety" (A.24, Personal Communication, March 2001).

Areas of importance

The perceived importance of security is highly dependent on the area being discussed. An opinion of security being very important holds true where nuclear materials are involved, especially at PFP and where there is a need to protect classified information. Important topics that were not mentioned were terrorism/physical threats, sabotage, and the protection of information (computer, business sensitive material.)

From responses to interview questions, it is apparent that people know, cognitively, the importance of security regardless of the level of commitment they demonstrate. Common responses to the need for security in their particular work areas were checking for badges and being aware of strange events and people. Although these are appropriate answers, they seemed to be rehearsed. There was a feeling that the interviewees were saying what they thought we wanted to hear, rather than demonstrating in-depth knowledge of commitment to security.

Physical/hazardous materials and classified information are definitely understood as needing security. But these are not issues relevant to the majority of workers. More focus should be spent concerning issues that pertain to the office/lab type worker. Perhaps some material should address the difficulty in keeping up with technology, especially electronic media; how acts of terrorism/sabotage can be committed from distant lands; repeat how a compilation of non-sensitive materials can tell the story of a classified document; and educate on the importance of information protection. When doing this, real-life examples should be used as often as possible.

Frustrations

Regarding employee compliance with guidelines, managers often said that their employees have “accepted ‘therefore’ adhere to what is required.” Some frustrations however, do exist. Some managers indicated that employees do not take security compliance seriously. Part of this problem could be the message that is sent by the manager. In general, managers do not feel that they would face consequences if their employees do not comply. Some said they would endure the same consequence as the employee, but most voiced their consequence would be a reduction in productivity. Still others stated their consequence would be “insignificant.” If managers have no incentive to comply or ensure that their employees are in compliance, they may not be adhering to or promoting the security message.

Frustrations could also be attributed to a perceived problem with security communication. One manager said his employees are frustrated with “their inability to grasp and be aware of expectations. This is due to inconsistencies and difficulty in understanding” (A.27, Personal Communication, March 2001). Suggestions to improve this problem were less cumbersome, simplified messages along with increased communication.

Competing for Time

If the security department indeed increased their communication to managers and strengthened their message, there would still be communication problems from the managers to the employees. Virtually all managers have extremely busy schedules and numerous tasks to accomplish, making everything come into competition with managing security. In areas, or within job titles, where nuclear material is dealt with regularly, there is high involvement with security. These people, particularly those located at the PFP, view security as extremely important and give it the attention it needs. The ideal answer was given by one individual who expressed that it is the duty of “management to make sure (employees) have the right attitude towards security” (A.25, Personal Communication, March 2001). This however is not the view of everyone. In less sensitive areas the purpose of security is not as well understood or valued. This puts security as a low priority. One manager informed us that “security is only about .5% of what he does” (A.28, Personal Communication, March 2001).

Value of Focus

Managers see badging, the protection of classified/sensitive information, the protection of special materials, and protection against the theft of government property to be the most important security focuses. On the other hand, they see little value in stressing “blanket procedures” that do not necessarily apply to everyone. An example of this is the HGET training. Everyone from labs to “hot” areas take the same computer-based training; however, not all of the same information should be given with the same emphasis in every area. “One size does not fit all” (A.15, Personal Communication, March 2001). Another qualm is “overkill” on some security topics, which can be counterproductive (A.14, Personal Communication, March 2001). An example is requiring employees to frequently change their computer password. This makes them hard to remember, forcing a person to write them down, which defeats the purpose. Again, this demonstrates a clear understanding of why physical materials are protected and a lack of reasoning for the significance of shielding intangible materials.

Management Involvement

To emphasize security awareness and ownership, collectively managers are currently reviewing procedures, discussing problems as they arise, occasionally bringing up security topics in meetings, and making employees who forget their badge bring donuts for the group.

Interviewees all feel that they have “pretty good” security awareness, and are knowledgeable in their responsibilities. Accompanying most of the responses was an “I know what I need to know for my job” attitude. However, there is always room for improvement and managerial suggestions to increase their awareness were more security presentations, more effort to test/challenge them, and improvements in training. Training was said to be too computer based now, which is quickly done by clicking past everything and taking the quiz without reading any of it. People choose which information they will attend to; if the media to get your message across is easily by-passed, there will be minimal attention.

Media

Recalls and Preferences

The majority of managers were able to recall having seen posters, web banners, web pages, and HGET. With some help, they remembered security e-mails, calendars, Security Ed., and mouse pads. Those tools that required help to remember can be said to be less effective, for numerous reasons. E-mails are easily ignored and calendars and mouse pads are not frequently changing; therefore, they are no longer being attended to. This can be tied to a popular marketing concept termed novelty. This notion explains that people need change to keep them attentive. Security Ed is only in the Hanford Reach, which does not appear to be widely read, and its aided recall was confused with security education itself. Preferences were expressed for visual media including videos, computer banners, and other computer-based media.

Perceived Effectiveness

Managers believe that HGET, computer training, communication by managers, and posters and web banners/pages that are frequently changed are the most effective types of media. But if posters and web banners are not constantly changing they will be the most ineffective. Research on billboards corroborates this concept. E-mails are also seen as ineffective because they are easily ignored.

To utilize security communication by managers, the security department must recognize and accommodate their busy schedules. If they had concise information to help them be knowledgeable and have a clear understanding of the message they would be more comfortable and willing to relay the security information to employees. Making time for security is not a high priority. This could be due to the following:

- Security education funding no longer comes out of the manager's budget
- Many do not recognize real consequences
- Its perceived importance is low in many Hanford facilities
- *Employees are not involved in structuring it.*

Content Analysis

The purpose of the content analysis is to characterize and evaluate for common themes, the messages and modes that are used to communicate security awareness within the Department of Energy (DOE). The review used documentation provided by Mr. Chester Braswell, security awareness coordinator at PTH. This included two broad classes of information: 1) sample communications collected by Mr. Braswell in the early 1990's from several of the sites throughout the DOE complex, and 2) recent samples of information currently being used at Hanford including Security Ed cartoons, and a DOE poster. In addition, Mr. Braswell has shared some of the other techniques he is using to improve security awareness and ownership at the Hanford site.

The team's experience spans the range from no previous training or experience with DOE to extensive training in DOE security requirements. In addition, some of the members have experience with industrial security programs.

The team used a Delphi analysis approach reaching general consensus on the following observations.

Communications Strengths

Use of Photographs

The document titled "Security System Bulletin" 2nd Quarter 1990, (Exhibit 1) includes photographs of workers, apparently from a laboratory facility (non-Hanford). The title of the photos reads "What is wrong with these photos? (Remember Laboratory Policy...)" The photos depict improper wearing of security badges. The photo was of poor quality in the copy but it was still possible to observe, that in one picture the individual was not wearing a badge and in the second picture a badge is being worn on the belt instead of above the waste.

There are several aspects that make these photos good communications tools.

- The conditions are obvious to an experienced worker, without reading the captions. However, the caption instantly reinforces individuals for having the right answer.
- A less experienced worker may get the left hand picture right but would perhaps be less sure of the problems in the right hand picture. The set of photos provide both neutral information and reinforcement through the personal challenge created by the title. The caption in the left hand photo tends to reinforce and provide information to the readers.
- The message in the left hand photo is very affirming: "If you noticed...you are very security conscious." This positive wording validates the reader so that if they do not recognize what is wrong in the right photo, there is not demeaning language to make them feel inadequate. Even if the reader doesn't know what is wrong there is no implied demeaning language.
- More subtly, the use of coworkers, people we may know, promotes acceptance of the requirement. They are smiling and may be well-liked and easily recognized

individuals at the facility.

Conveying a Message of Respect

The tone of the article in this document (Exhibit 1) titled “Security Infractions” is excellent. It is informative (cognitive) and suggests ways of coping with unusual situations that often lead to security infractions. It focuses on "right" behaviors and helps individuals recognize the conditions that can lead to mistakes in security protocols. The program uses positive terms such as “double-check team” that send a message of dependence on each other to help maintain security discipline. The last sentence reads, “BE YOUR OWN DOUBLE-CHECK TEAM IF YOU ARE ALONE. This statement projects a respect to the security worker that helps the reader accept coaching.

Cartoons with Simple Message

There are two cartoons that seemed to have very simple, easy to understand messages (Exhibit 2 and 3). Another strength of these cartoons is that the picture and the words appear to support each other. The first has a caption, “Pull together, security is everyone’s job.” The message is more positive in the first cartoon - people working together to accomplish a task (Exhibit 2). The second is captioned, “It only takes one of us to bring all of us down.” It depicts a strong relationship between personal action and protecting national security by using an image of falling dominoes. The first domino to fall is individual security. This sends a cognitive message that security depends on individual actions (Exhibit 3).

Attention-Getting Signs

Mr. Braswell has found special plastic prism materials that allow him to make animated signs that he plans to use on safes and near security room doors to remind workers to verify that drawers and doors are locked. These signs could be effective because they provide helpful reminders with visual movement that catches the eye. They are helpful reminders that may prove to be good aids to the workers. His desire to help individuals be successful by creating new and better tools such as these, demonstrates a level of caring and concern for his intended audience.

Useful Gifts

Another tool that Mr. Braswell has used is a mouse pad with a photograph of some radiological work that is taking place at the tank farms at night. The lighting of this night operation seems to highlight the nuclear worker. Only nuclear workers wear the characteristic yellow hooded clothing shown in this photo. The picture communicates a sense of pride in having the ability to safely work with this highly hazardous material. People at the site will likely identify closely with the tone of competence, the dedication and the sacrifice implied by the shift worker doing Hanford work at night in the tank farms. Mr. Braswell has encircled the mouse pad with a security message, which may not be recalled, but is always on the users desk top and provides a constantly available reference to the Security Training Program website should the individual have a need to

find out something about security. Although the words may not be memorable, the “gift” from security education program probably has a long residence time.

Rewards for Security Behaviors

Mr. Braswell has made an effort to identify small but valued "prizes" for individuals who exhibit positive security behaviors. These rewards include a flashlight and a utility tool like a leatherman. This element reinforces good behaviors.

Communications Detractors

There were three detractor categories identified:

- 1) A **“parent-child” form of communication** that talks down to the readers, uses controlling language and threats, both direct and implied. The difference between the message in the “Security System Bulletin” (Exhibit 1) and the “Security Bulletin,” (Pantex January, 1989 and March 1990) (Exhibit 4 and 5 respectively) is obvious. The Pantex documents use underlined words to emphasize things that must be done and assign responsibility to the individual. The article titled “Security Infraction in the March edition (Exhibit 5) says, “Our security infraction record for FY-90 is not one to be proud of.” There are messages that seem to show that the security program doesn't trust workers. These parent-child communications include statements such as “Security inspectors on duty...have been instructed to check employees to assure they wear seat belts” and “Security inspectors will spot check vehicles to assure keys are not being left in them when unattended... When keys are found... they will be taken to security headquarters where the operator...will have to claim the keys.” The banner of this bulletin says the purpose is to provide topics of interest that can be posted and used by supervisors. The opening line of the bulletin starts with “Supervisors must share information... with all employees.” The language is controlling, punishing, and demeaning. It appears to assume that individuals, even supervisors must be “policed” into doing the right things. This approach might get compliance but does not appear to engender commitment and ownership.

Similar examples of demeaning language included in the Hanford Security Education Council's Poster titled “I believe we don't have a security problem.” (Exhibit 6) The poster yells “DON'T BE NAÏVE” and implies that if you disagree with security requirements (and the Security Council) you are as foolish as a child believing in the Easter Bunny. This “if you don't agree with us you are stupid or childish” implication is a recurring theme in much of the DOE security communications and often appears in cartoons. In one of the Security Ed cartoons, Ed uses the term “meathead” (Exhibit 7) to describe people who exhibit unacceptable security behaviors. In this cartoon Ed asks the question, "You know what ASSUME means don't you?" The question probably elicited a conditioned response from someone who has heard the question before and was told it meant, "it makes an ass out of u and me." But if they didn't respond that way, the mouse reminds them to think about. Both messages, the one stated and the one hinted at are personally negative. Another cartoon image (Exhibit 8) is an ostrich sticking its head into the sand with the caption

"Don't be in the dark about security." This is another example of a "don't be stupid" message that alienates the reader from the message.

A Ford Aerospace document titled "Security Awareness" (Exhibit 9) includes the letter "U" that has eyes that are looking out from the word. The almost subliminal "eyes on you" message is reinforced with the image of a spy satellite looking down from above. The message seems to be that we have our eyes on you. The first line of the second page of this document says "Uncle Sam has done some checking up on you and decided that you are a trustworthy person." This opening line to a newly cleared person appears to make it clear that the individual is found to be trustworthy because they meet "Uncle Sam's" criteria. An implication of this statement might be that if you do not have a clearance, you are not trustworthy.

The rewards that are given out by managers (the Hanford security reward program) could be perceived by workers to be an attempt to bribe or control their behavior. This is consistent with perception that there is a parent-child relationship. If workers are empowered and encouraged to give these rewards to their coworkers who exhibit strong security commitment, the program would probably be less likely to be perceived as being manipulation by managers. It is not clear how the rewarding is currently being managed. This is a potential area for further review, especially by the WSU-Vancouver research team.

- 2) **Complex, inconsistent, or incongruent messages.** The use of humor in cartoons can send a very confusing message, especially when placed in juxtaposition with the negative messages that may be included in the written articles by the same organization. In many cases the cartoon pictures (Exhibits 10) don't clarify or support the text message. In other cases the message is unclear about how it applies to security. The Security "ED" cartoons are generally more effective, having graphics that match the message, however the (Exhibit 11) messages are often quite long or require much interpretation in order to understand them. This can be good, but may lose some of the readers. For example in this cartoon there is a man opening a package with a caption about letting the experts inspect packages. The message appears to be based on "suspect package" issues. It took several moments of studying the cartoon before the message was understood.

In the "Security Bulletin" November 1988 (Exhibit 12), the lead article indicates there will be a "security awareness week" coming soon and invites all employees to visit some displays that will be set up. The December 1988 edition (Exhibit 13) the lead article uses a similar title but starts off as follows: "All employees must be scheduled to attend an annual security refresher..."

- 3) **Use of cognitive messages:** There is a nearly singular reliance on cognitive messages presented in text and logic. The Boeing Calendar (Exhibit 14a-g) is a good example of a well-communicated cognitive message. The calendar provides some examples of individuals referred to as "Most Unwanted" that have committed acts of espionage. The layout is excellent. The description of the events is interesting. And, the message is clear. But it appears there are no strong emotional appeals in the

narratives. The emotional response to the article is neutral. This lack of emotion reaction could reduce the learning and retention of the underlying message. It would appear to be the author's intent to have the reader identify characteristics that could predict that some espionage activities may be occurring. There are many examples of cognitive appeals being made. The article titled "The Counterintelligence Viewpoint" (Exhibit 15) represents one of them. These messages appear to be tailored to ensuring that the work force understands the security requirements, but do not do a good job of engaging the reader's commitment because they communicate on an intellectual rather than affective level. In many cases the message is one of "what is expected" without providing a justification or sense of importance for the required action.

General Conclusions

This review concludes that strong positive messages are perceived when programs:

- Validate individuals
- Portray workers as members of a security team striving toward a common goal
- Use positive reinforcement for good behaviors
- Keep messages simple and direct
- Strive to send a consistent message that workers are valued, trusted, and relied upon

In contrast, programs create barriers to building awareness and ownership when messages are:

- Perceived to be demeaning
- Rely on guilt or punishment
- Threaten individuals directly or indirectly

It is likely that security experts who are preparing the messages are unaware that they have assumed the "parent role" in their relationship with the workforce. The method and messages used to communicate expectations and influence security commitment have an important impact on the likelihood of success. The communications that have been used may be able to achieve compliance when security is present in the workplace, but they do not appear to be effective at building the desired ownership and internal commitment to security sought by the security trainers. The resulting negative reactions and lack of commitment can elicit responses that range from poor retention of security information to willful noncompliance with important aspects of the security program.

Most of the messages that were reviewed relied on an intellectual approach with very little emphasis on emotional appeals. This approach may not build the desired levels of commitment or achieve the desired behaviors.

This review did not consider recent security articles in the Hanford Reach that may show a more positive attitude toward the workers. By reviewing the early 1990's security communication materials, it has helped the team better understand how the mixed

messages of the past may be contributing to some of the misunderstandings and resistance of the workforce toward security.

Security System Bulletin

Security and Safeguards ♦ Safeguards Assurance ♦ Operations Security ♦ Internal Security

Vol. 5, No. 2

2nd Quarter 1990

Security Infractions

by George VanTiem, OS-10

A break in routine or an interruption can often cause a security infraction. Awareness that these occur and mitigating actions to prevent infractions are necessary. Many security infractions may be traced to the following deviations from routine:

- An employee is absent from work or leaves early. Absenteeism and leaving early may cause security problems. Others should be made aware of proper security procedures in your absence. If you intend to leave early, plan for it. If another employee must leave hur-

riedly because of medical reasons or an emergency, check that employee's work area.

- The routine of placing classified documents or material in a repository and locking it is interrupted by a visitor or a phone call. Two basic rules should be followed if this situation should arise. If the telephone rings while you are placing your classified matter in a repository and locking it up, either

(1) hold onto the classified matter while you answer the telephone, or (2) answer the telephone, put the caller on hold immediately and finish what you are doing. If your routine is interrupted by a visitor, ask them to wait one moment while you finish storage of the classified matter.

- The other half of the double-check team is absent. Advise your supervisor if this occurs and arrangements have not been made to assign an alternate monitor. It should be the responsibility of the monitor to find another employee to assume monitor duties if they are going to be absent.

- An employee works alone outside normal working hours. If you are the only employee on the premises, it may be prudent to finish your classified work earlier than usual. Allow yourself a few extra minutes to make sure the documents or material you are working with are stored properly and that all of them are properly secured. **BE YOUR OWN DOUBLE-CHECK TEAM IF YOU ARE ALONE.**

What is wrong with these photos?

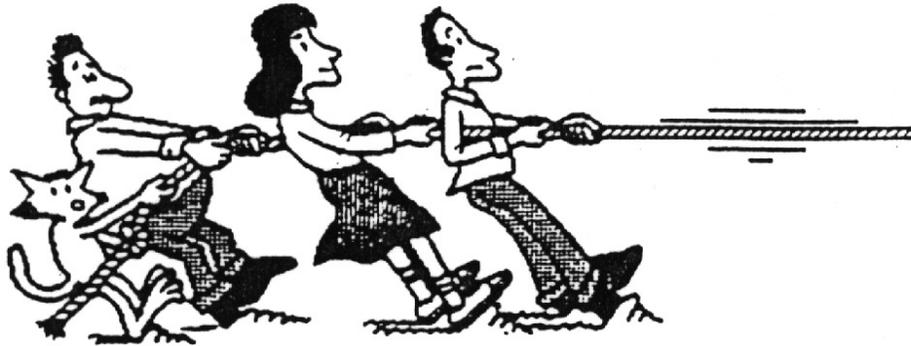
(Remember Laboratory policy...)



If you noticed that the person on the right is not wearing a badge, you are very security conscious. Individuals must wear their badge (cleared and uncleared) at all times on Laboratory property.

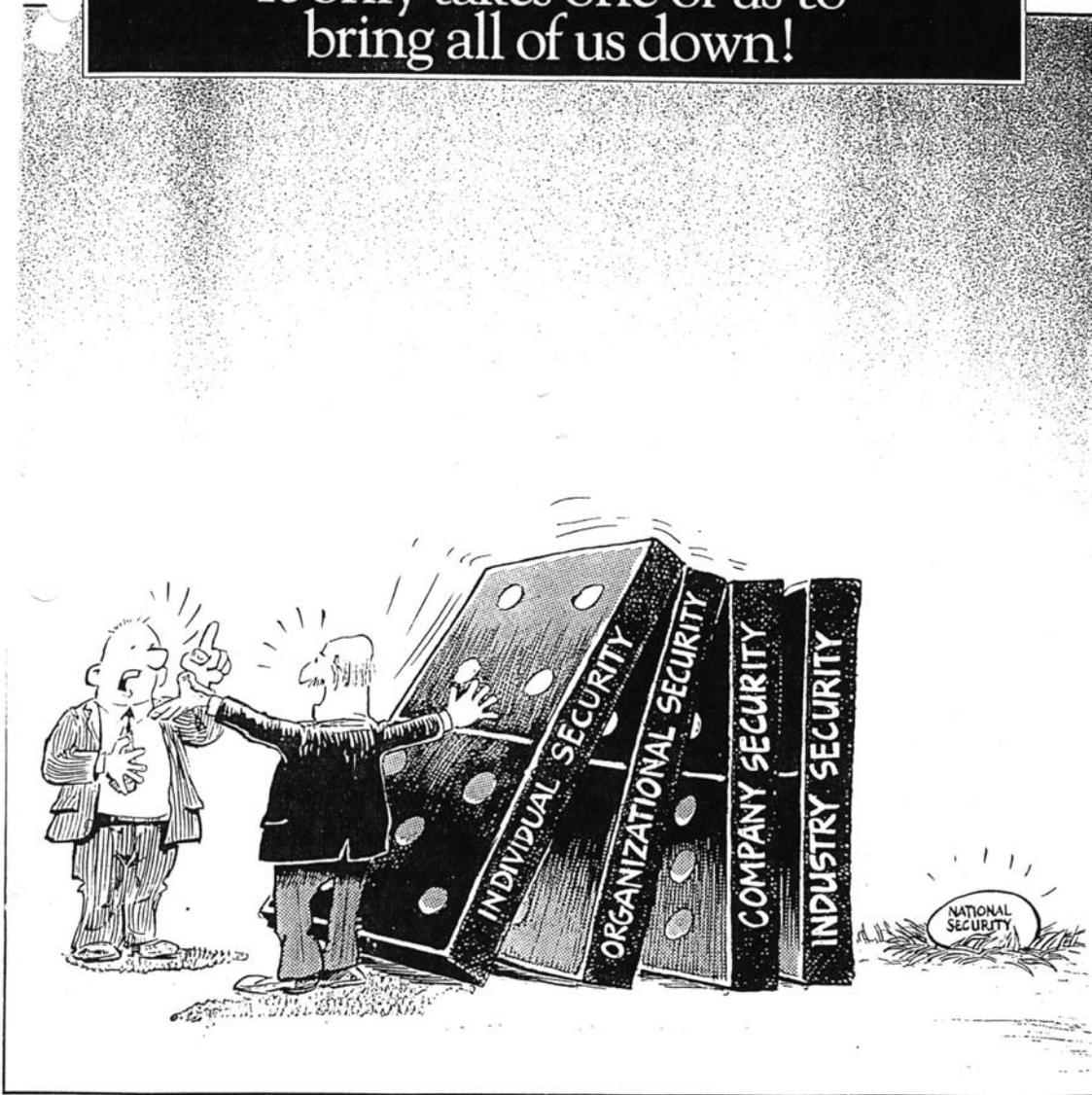


Both individuals are wearing their badge incorrectly. The proper way to display your Laboratory badge is to wear it in plain view, above the waist, and with the photo outward at all times.



*Pull Together,
Security is
Everyone's Job*

It only takes one of us to
bring all of us down!



1991 SECURITY AWARENESS

THIS IDEA CREATED BY CLASSIFIED CONTROL EMPLOYEES/4-8249/SEATTLE,WA

SECURITY BULLETIN

January, 1989



THE PURPOSE OF THE SECURITY BULLETIN IS TO PROVIDE TOPICS OF INTEREST AND CONCERN. IN ADDITION TO BEING POSTED IN A CONSPICUOUS PLACE, ACCESSIBLE TO ALL EMPLOYEES, IT MAY BE USED IN SAFETY MEETINGS

PANTEX

Supervisors must share information contained in this bulletin with all employees as indicated above.

---SECURITY INFRACTIONS 1988---

CY 1988 has, come and gone, and whether it was a good or bad year is left to individual interpretation. Security wise, it was a fairly good year as we had 19 security infractions compared to 23 in CY 1987. This improvement was brought about by security conscientious employees and your efforts are appreciated. By working together we can further reduce the number of security infractions in CY 1989.

VEHICLE KEYS

Vehicle keys must not be left in government vehicles when unattended. From a security standpoint, we simply cannot take the chance of providing an adversary, either an insider or outsider, the opportunity to use a government vehicle against us in an effort to accomplish their mission. From a Safety standpoint, keys shall not be left in unattended vehicles. Safety Standard #318, which has been revised and will be published soon, states: No vehicle will be left running and unattended with the exception of firefighting equipment. This equipment will have chocks placed in front and rear of the wheels.

Remember, it is not impossible for a vehicle to accidentally slip into gear, causing the vehicle to move and possibly strike someone or something, causing serious injury and extensive damage to other equipment, structures and to the vehicle.

Security Inspectors will spot check vehicles to assure keys are not being left in them when unattended. When keys are found in vehicles, they will be picked up and taken to Security Headquarters where the operator of the vehicle will have to claim the keys.

SECURITY BULLETIN



MARCH 1990

PANTEX

THE PURPOSE OF THE SECURITY BULLETIN IS TO PROVIDE TOPICS OF INTEREST AND CONCERN. IN ADDITION TO BEING POSTED IN A CONSPICUOUS PLACE, ACCESSIBLE TO ALL EMPLOYEES, IT MAY BE USED IN SAFETY MEETINGS.

PROPER WEARING OF IDENTIFICATION BADGES

Several reports have been received regarding employees not wearing their I.D. Badges. Your badge should be worn at all times while on the plant site and must be worn at all times when in a security area. Badges will be worn on the outer most clothing or on a neck chain above the waist with picture facing out. If you observe any employee or visitor in a security area without their I.D. badge properly displayed it is your responsibility to challenge that individual and ask to see their I.D. badge. If they are unable to produce a valid I.D. badge call security immediately.

SECURITY INFRACTION

Our security infraction record for FY-90 is not one to be proud of. We have recorded nine security infractions during the period October 1, 1989 through February 28, 1990. Be aware, help prevent Security Infractions.

USE OF SEAT BELTS

All employees are responsible for wearing seat belts when operating or riding in government vehicles. If personal injury results from an accident in a vehicle equipped with seat belts and an investigation reveals that seat belts were not in use will be considered contributory negligence on the part of the driver or passengers. Reference Safety Standard 318, paragraph g. (2).

Security Inspectors on duty at Guard Stations have been instructed to check employees to assure they are wearing seat belts. If they are not, Security Inspectors will ask the employee(s) to wear their seat belts in compliance with Safety Standard 318.

The above in no way, alters the use of seat belts by Security Personnel as outlined in the interoffice memo published January 10, 1990.

I Believe We Don't Have A Security Problem.



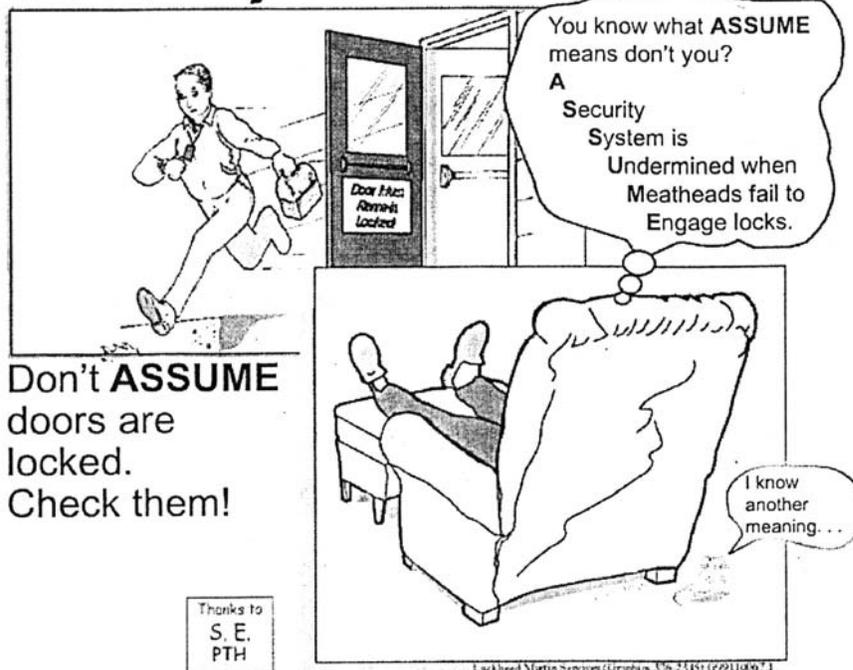
- I believe we're making mountains out of molehills.
- I believe our programs don't interest our competitors.
- I believe we're wasting time securing sensitive documents against theft.
- I also believe in leprechauns, tooth fairies, the Easter Bunny...

DON'T BE NAIVE. Protect Hanford Security.

Sage Intermunity Removed

Hanford Security Education Council

Security Ed



Make sure doors close properly

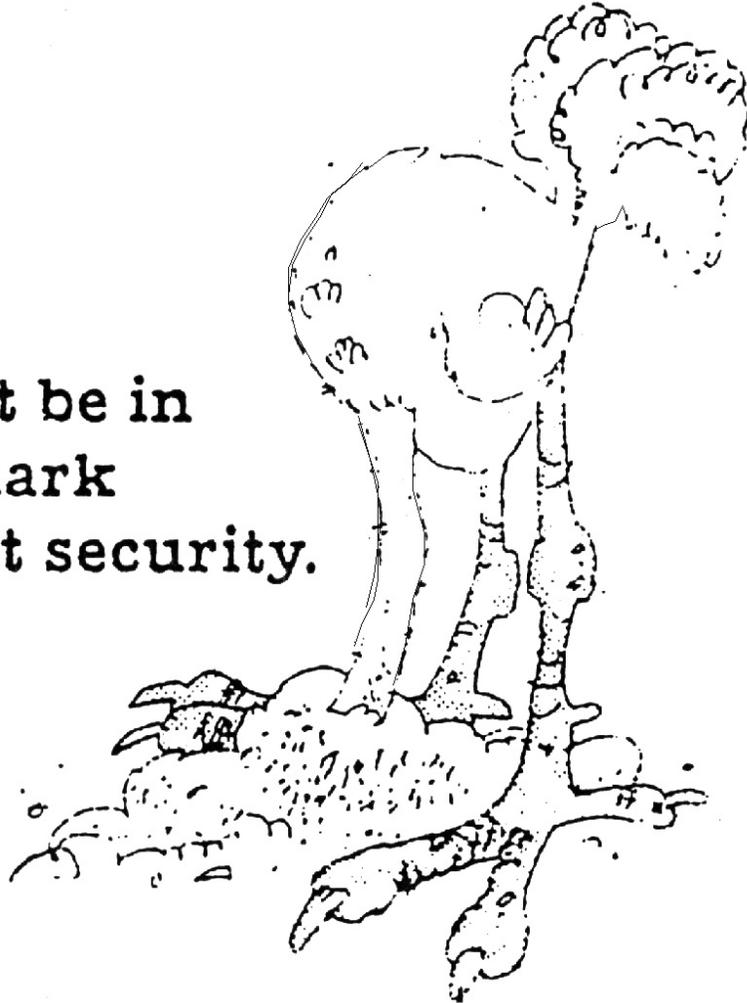
With more than 1,000 facilities on the Hanford Site, and more than 15,000 people with Site access, it is not hard to imagine that unsecured doors are a serious problem. Quite often, the doors to these unsecured facilities are locked, but air balance or a faulty door closure assembly prevents the door from closing completely.

The number of buildings found unsecure by Hanford Patrol is increasing. This is unacceptable, and all of us must heighten our security awareness and ensure our workplaces are not compromised.

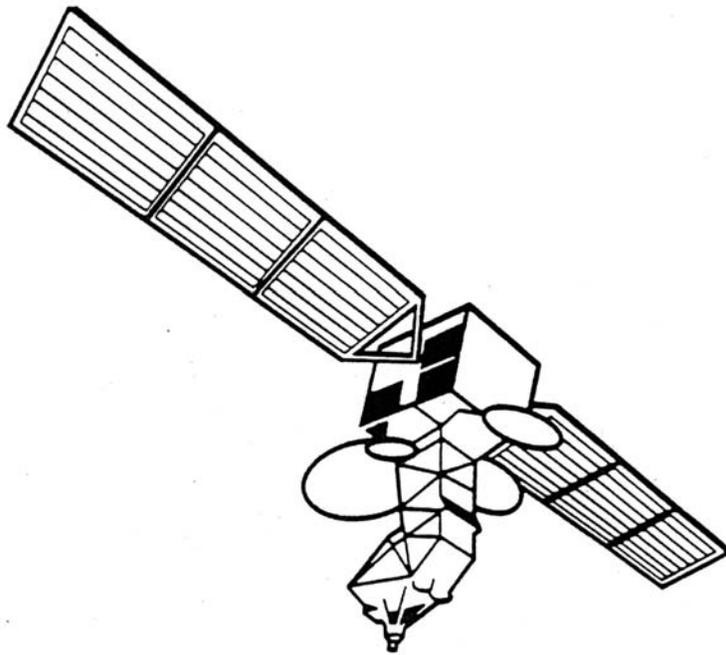
Your constant vigilance is needed to ensure that your facility remains safe and secure. Each time you pass through a locked door, make sure it shuts tight. To increase awareness, the Protection Technology Hanford Security Education office created posters like the one shown here as reminders to employees concerning security issues.

To obtain the latest poster, visit the PHMC SAS Web site at <http://www.rl.gov/sas/pg1posters.htm>. ♦

**Don't be in
the dark
about security.**



SECURITY AWARENESS



NEWLY CLEARED EMPLOYEE INDOCTRINATION
Presented by Your WDL Security Education Office

 **Ford Aerospace & Communications Corporation**

BASIC PROTECTION OF CLASSIFIED MATERIAL
AN INTRODUCTION FOR THE NEWLY-CLEARED PERSON

or

Everything you never wanted to know about classified material
but were afraid we'd tell you!

*** CONGRATULATIONS! ***

Uncle Sam has done some checking up on you and decided that you are a trustworthy person. You have, therefore, been given authorization to have access to classified information. Wonderful....your're thinking. Now what?

For those of you who may still think having a clearance is a terrific status symbol, we'd like to take this opportunity to squash that illusion! Here's a better way to think of it.

Uncle Sam has just given you a big burlap bag. Every time you get a piece of classified information, every time you acquire another access, imagine that you are adding a brick of RESPONSIBILITY to that bag! And that it's yours to drag along with you everywhere you go. Forever!

So, you can see that having a clearance is not something to be taken lightly. It is a privilege, and there are duties and obligations which are an integral part of that privilege. What follows is an explanation of just what you've gotten yourself into!

*** WHAT IS CLASSIFIED INFORMATION? ***

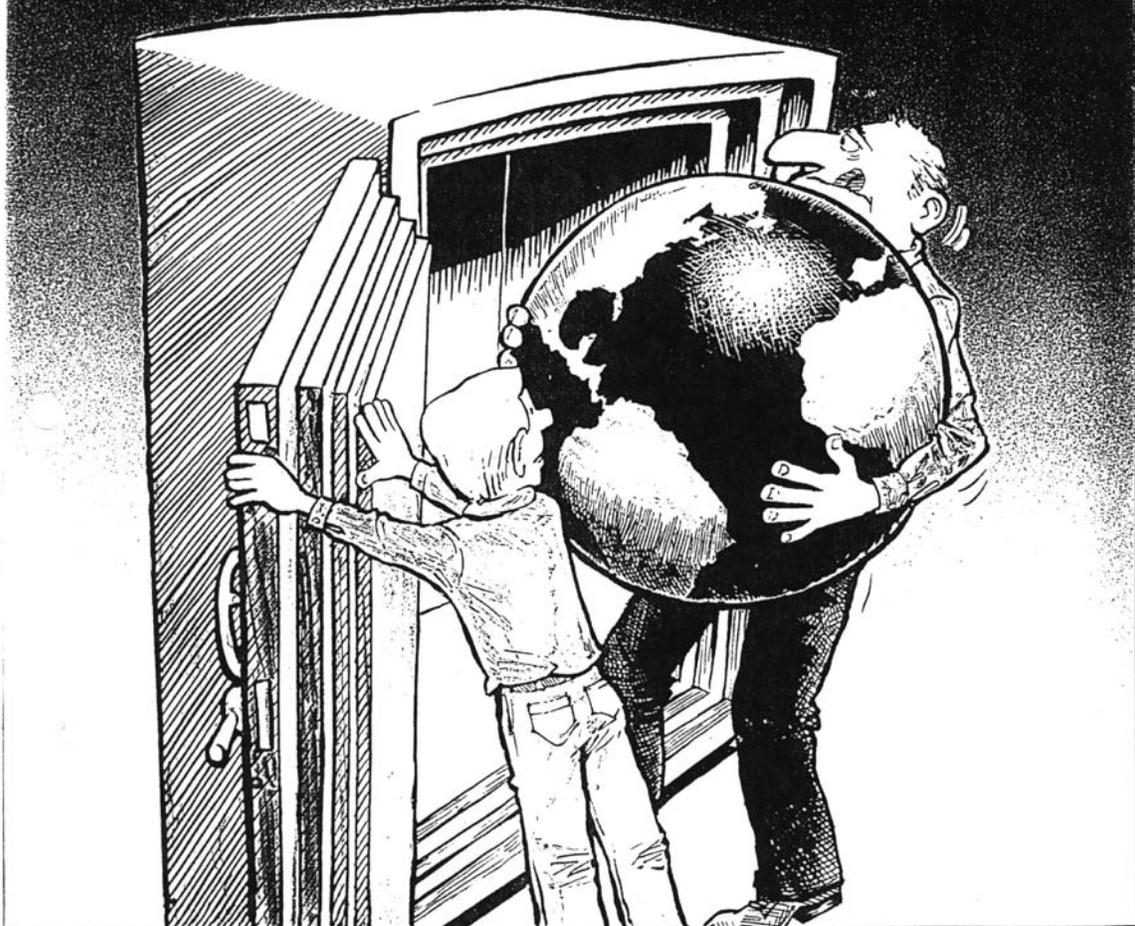
A DEFINITION

The "official" definition goes something like this:

It is information or material that is: (a) owned by, produced by or for, or under the control of the U.S. Government; (b) determined under E.O. 12356 or prior orders to require protection against unauthorized disclosure; (c) and is so designated.

Whew! That's quite a mouthful. Translation is relatively simple. Classified information is anything Uncle Sam says it is, and it will be marked as such. You will know when you're handling classified information! All documents will be marked. They have special cover

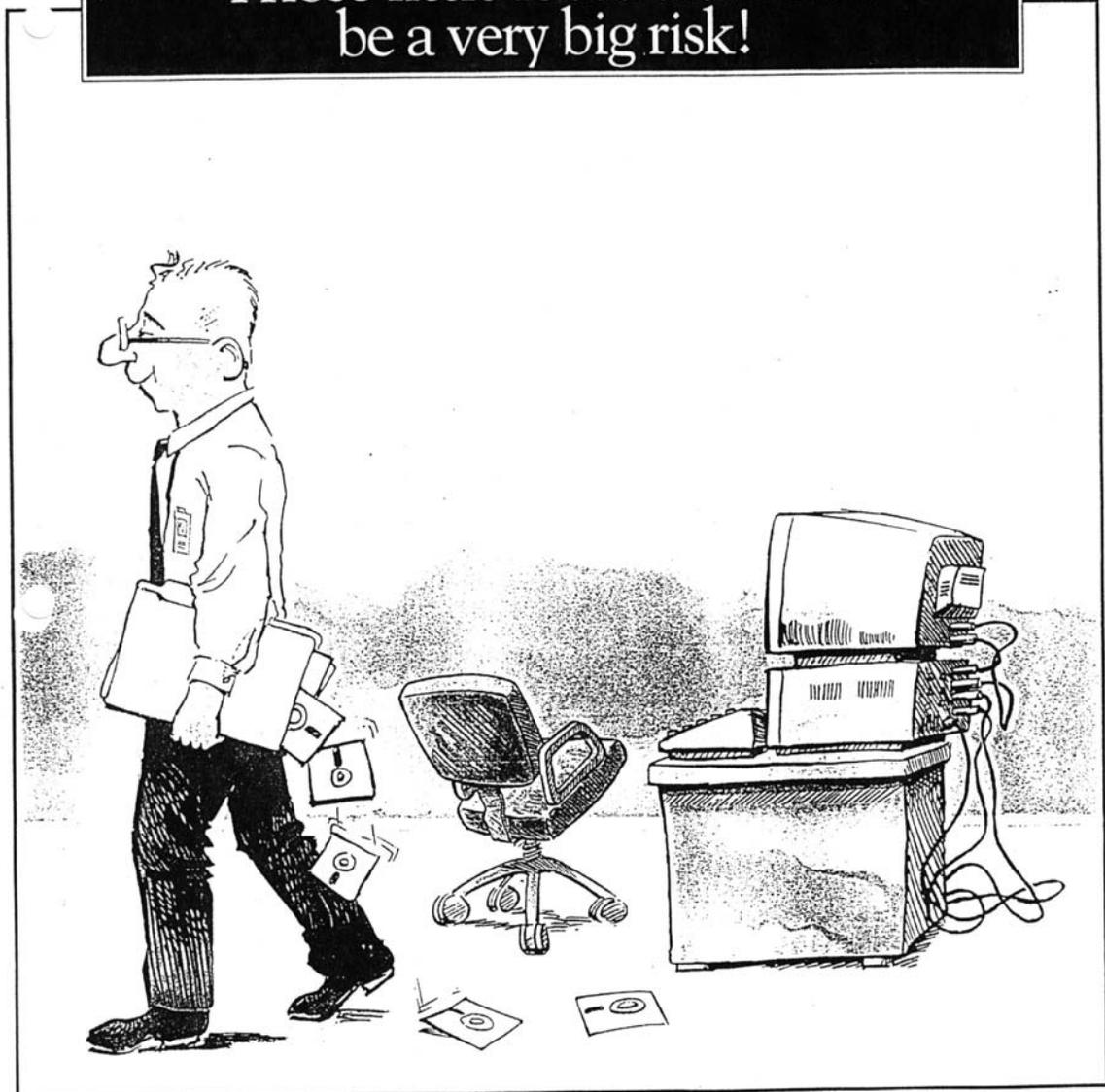
Practicing good security will
keep our world in safe hands!



1991 SECURITY AWARENESS

THIS IDEA CREATED BY KENNETH W. HARRISON/K-1700/OAK RIDGE,TN

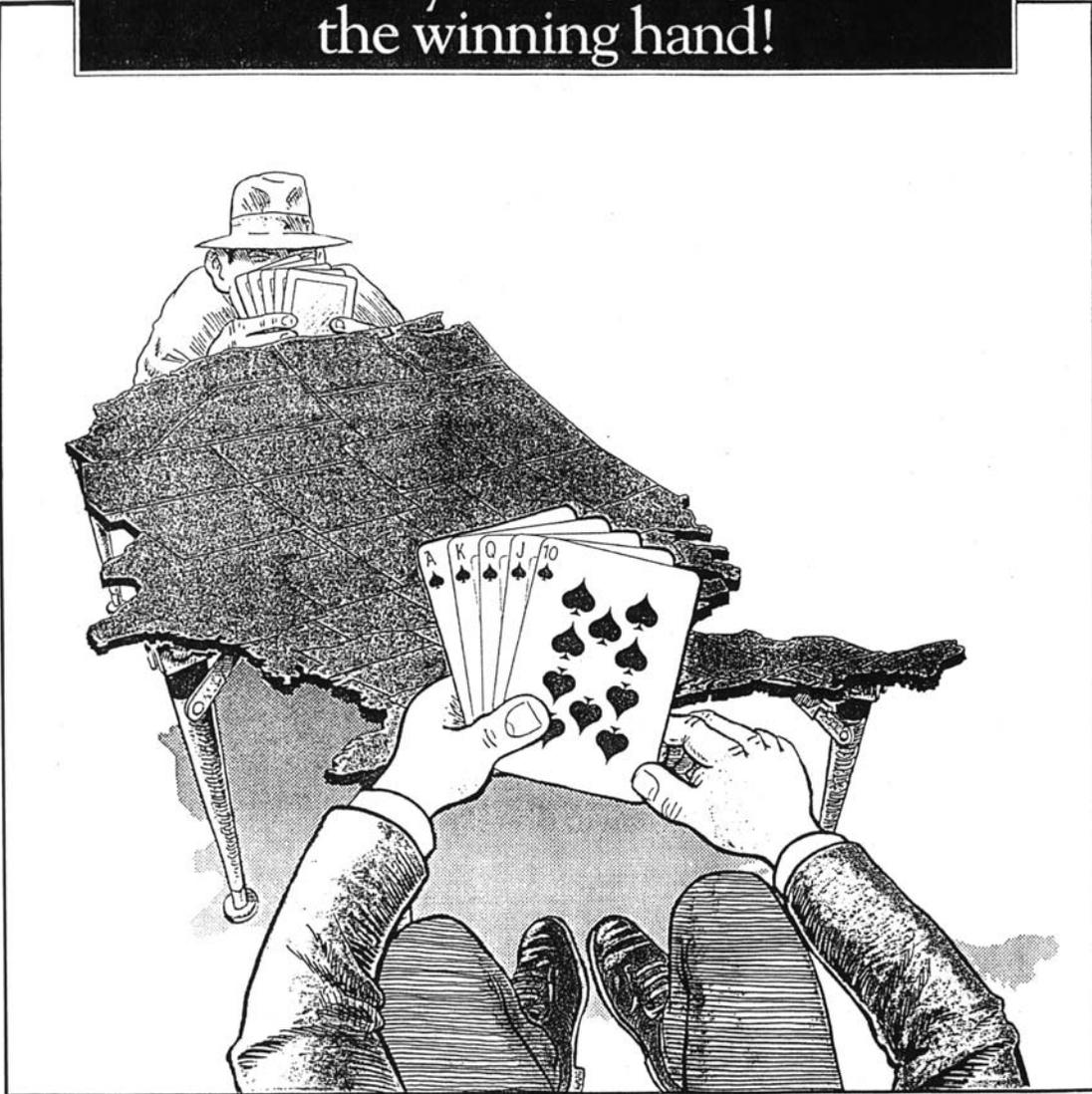
Those little loose disks can
be a very big risk!



1991 SECURITY AWARENESS

THIS IDEA CREATED BY GREGORY KING/3-9325/WICHITA,KS

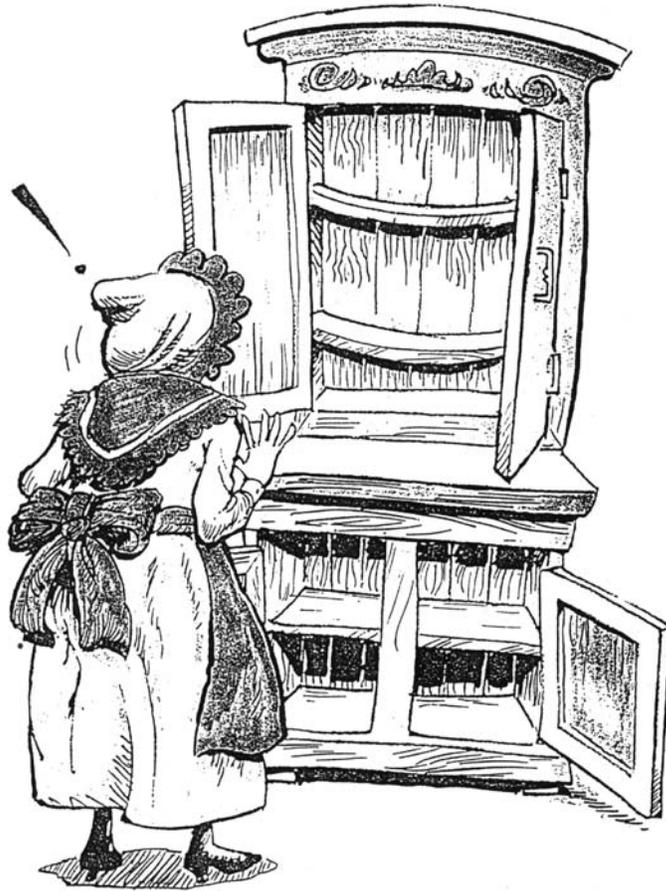
Security deals our nation
the winning hand!



1991 SECURITY AWARENESS

THIS IDEA CREATED BY W. JIM HAWN/K-1700/OAK RIDGE,TN

Ol' Mother Hubbard, forgetting a lock, went
back to her cupboard and right into shock!



1991 SECURITY AWARENESS

THIS IDEA CREATED BY CAROL MCPHERSON/2-2976/SEATTLE,WA

Security Ed



Don't forget to send your ideas for Security Ed to: Security Education, L4-09, or e-mail them to ^Security Education PHMC. If your idea is used, you will receive a credit line in the *Hanford Reach* and will become eligible for prizes in the "Security Pays in Many Ways" campaign.F

Tank-farm contractor renews safety commitment

The managers at CH2M HILL Hanford Group want employees to know the managers are serious about safety issues. Serious enough to dedicate an entire day to promoting safety awareness and conveying the priority managers place on safe work practices.

"This is an opportunity for the whole company to step back and really take stock of how and why we do things," said Fran DeLozier, CH2M HILL Hanford Group president and general manager. "It's called Communicate the Commitment Day because that's exactly what we want to do."

Employees will take a day away from their normal work schedules June 16 to participate in safety modules ranging from injury reduction to conduct of operations to playoffs of the Jeopardy-like game used

in ISMS training. A catered lunch will be served by CH2M HILL managers.

To help promote more interaction and feedback among managers and workers, CHG managers will talk informally with employees and answer questions during the lunch break. The day will end with an all-employee meeting to discuss the company's recent successes and some of its upcoming challenges.

"We want this to be a meaningful, enjoyable event," DeLozier said.

The Communicate the Commitment Day will be held at Richland High School from 7 a.m. to 3:30 p.m. on June 16. ♦

SECURITY BULLETIN

November, 1988



THE PURPOSE OF THE SECURITY BULLETIN IS TO PROVIDE TOPICS OF INTEREST AND CONCERN. IN ADDITION TO BEING POSTED IN A CONSPICUOUS PLACE, ACCESSIBLE TO ALL EMPLOYEES, IT MAY BE USED IN SAFETY MEETINGS.

SECURITY AWARENESS WEEK

December 5-9, 1988 has been designated as Security Awareness Week at Pantex Plant. In addition to the annual Plantwide Security Briefing, the Protective Force and Training Branches of the Security Force Department will have a security equipment display and a video tape presentation of the annual DOE Pistol Tournament and Inspector of the Year activities set up in the cafeterias during the week. We invite all employees to go by and review the displays, tape, and to visit with Security personnel who will be available to answer questions regarding the equipment and tape.

THEFT OF GOVERNMENT PROPERTY

The following law applies to all employees and pertains to any Government property including items such as office supplies, safety shoes, clothing, etc.

Whoever embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof, or any property made or being made under contract for the United States or any department or agency thereof - - shall be fined not more than \$10,000 or imprisoned not more than ten years, or both; but if the value of such property does not exceed the sum of \$100, shall be fined not more than \$1,000 or imprisoned not more than one year, or both.

SECRET WORK SHEETS

Secret work sheets or drafts, including photos, must be put into accountability or destroyed within sixty (60) calendar days after inception in accordance with Security Standard 485.09, Paragraph 4.b. Also, an "Accountability Log" showing all transactions, description of work sheet/draft, date initiated, by whom and date and signature of two persons performing the destruction, will be maintained by the department involved.

MAILING CLASSIFIED DOCUMENTS IN PLANT

When Secret documents are transmitted within the Plant, verification that the recipient is on the Authorized Custodian List for Classified Documents, published by the Classified Mail & Records Section, is required. Classified documents (Confidential or Secret) may only be transmitted on a need-to-know basis.

--- NATIONAL SECURITY IS OUR BUSINESS ---

SECURITY BULLETIN



DECEMBER, 1988

THE PURPOSE OF THE SECURITY BULLETIN IS TO PROVIDE TOPICS OF INTEREST AND CONCERN. IN ADDITION TO BEING POSTED IN A CONSPICUOUS PLACE, ACCESSIBLE TO ALL EMPLOYEES, IT MAY BE USED IN SAFETY MEETINGS

DON'T FORGET - SECURITY AWARENESS WEEK, DECEMBER 5-9

All employees must be scheduled to attend an annual security refresher briefing during the week of December 5-9. The Protective Force and Training Branches of the Security Force Department will also have a security equipment display and video tape presentation set up in the Plant Cafeterias during the week. All employees are invited to review the displays, tape and visit with Security Personnel who will be available to answer questions concerning the equipment and tape.

GUARDED CONVERSATIONS

We tell you not to talk about Pantex activities with your family and friends, then you go home and read all about it in some publication or hear about it on TV or radio. It just doesn't seem to make sense, does it? Well let's take a look at the reason for our policy.

If you were to ask a large group of Pantex employees to describe their job activities in an unclassified manner, they would probably do just that. Now, combine all those job descriptions and you could have an accurate detailed description of what goes on at Pantex.

This is the reason we can not afford to discuss our jobs with those who do not have a need to know. Probably your discussion would not be classified, but when combined with information that has been officially released it could very well be classified.

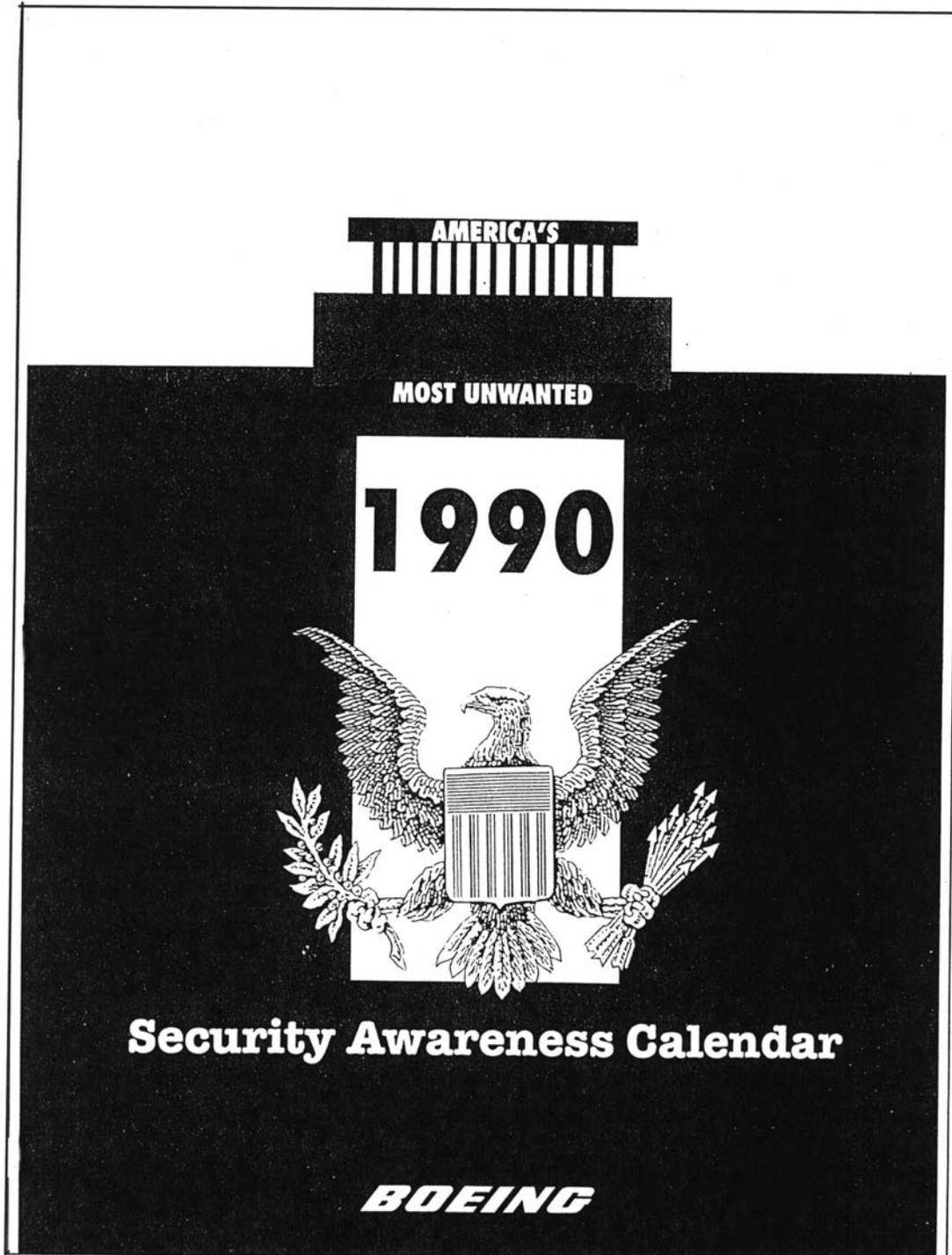
The best policy is not to volunteer any information. If it has been published, don't elaborate on it. Neither confirm or deny any published information. Press releases are carefully worded to prevent the release of classified or sensitive information that could prove detrimental to our security interest. You just can't afford to discuss your activities at Pantex and fail to maintain good security practices.

CHRISTMAS PACKAGES

Wrapped, unexamined Christmas packages will not be permitted in security areas [REDACTED]. Food containers taken into any security area are subject to search. Christmas baskets will not be allowed in any security area.

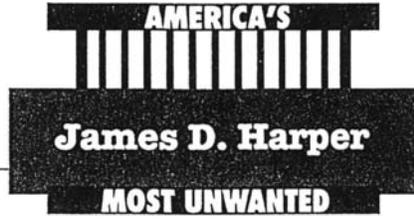
A HAPPY, SAFE, AND SECURE HOLIDAY SEASON TO ALL

--- NATIONAL SECURITY IS OUR BUSINESS ---



JANUARY 1990

1	MONDAY	<i>New Year's Day</i>
2	TUESDAY	
3	WEDNESDAY	
4	THURSDAY	^s
5	FRIDAY	
6	SATURDAY	
7	SUNDAY	
8	MONDAY	
9	TUESDAY	
10	WEDNESDAY	
11	THURSDAY	^s
12	FRIDAY	
13	SATURDAY	
14	SUNDAY	
15	MONDAY	<i>Martin Luther King, Jr. Day</i>
16	TUESDAY	



EMPLOYMENT AT TIME OF ESPIONAGE:

Electrical Engineer (Self-Employed)

CONVICTION DATE / SENTENCE:

May 1984 - Life imprisonment with the recommendation that he not be considered for parole.

INFORMATION COMPROMISED:

Extremely sensitive information on Ballistic Missile research and development programs in the United States. He obtained this classified information from his wife Ruby Louise Schuler, executive secretary to the president of Systems Control, Incorporated (SCI). After obtaining the classified information, James sold it to the Polish Intelligence Services (PIS). Loss of the documents has been determined by U.S. defense experts as "Beyond Calculation."

MOTIVATION:

Money

ESPIONAGE THAT COULD HAVE BEEN STOPPED IF THIS ADVERSE INFORMATION HAD BEEN REPORTED:

17	WEDNESDAY	
18	THURSDAY	\$
19	FRIDAY	
20	SATURDAY	
21	SUNDAY	
22	MONDAY	
23	TUESDAY	
24	WEDNESDAY	
25	THURSDAY	\$
26	FRIDAY	
27	SATURDAY	
28	SUNDAY	
29	MONDAY	
30	TUESDAY	
31	WEDNESDAY	

Excessive Financial Difficulties
 Unexplained Affluence - "Rich Lifestyle"
 Frequent Unexplained Trips Overseas

Report "Adverse Information"
regarding cleared personnel
to Security
 (see inside back cover).



**Prevent Security
 Leaks**

FEBRUARY 1990

1	THURSDAY	\$
2	FRIDAY	
3	SATURDAY	
4	SUNDAY	
5	MONDAY	
6	TUESDAY	
7	WEDNESDAY	
8	THURSDAY	\$
9	FRIDAY	
10	SATURDAY	
11	SUNDAY	
12	MONDAY	<i>Lincoln's Birthday</i>
13	TUESDAY	
14	WEDNESDAY	<i>St. Valentine's Day</i>
15	THURSDAY	\$
16	FRIDAY	



EMPLOYMENT AT TIME OF ESPIONAGE:

U.S. Air Force, Administrative Clerk

CONVICTION DATE/SENTENCE:

August 1986 - Bruce was sentenced to 25 years imprisonment, reduced to lowest rank in the U.S. Air Force and given a dishonorable discharge.

INFORMATION COMPROMISED:

None. Bruce was arrested by the FBI and U.S. Air Force Office of Special Investigations, while attempting to sell classified USAF documents concerning the SR-71 "Blackbird" reconnaissance aircraft to the Soviets. The FBI and U.S. Air Force Office of Special Investigations had received prior information of the event and initiated a counterintelligence operation targeted against Bruce.

MOTIVATION:

Money: Expected \$160,000 for Espionage Activity
Pay for Repossessed Car
Wanted to be a "long-term" agent for Soviets

117	SATURDAY	
118	SUNDAY	
119	MONDAY	Washington's Birthday
120	TUESDAY	
121	WEDNESDAY	
122	THURSDAY	
123	FRIDAY	
124	SATURDAY	
125	SUNDAY	
126	MONDAY	
127	TUESDAY	
128	WEDNESDAY	Ash Wednesday

ESPIONAGE THAT COULD HAVE BEEN STOPPED IF THIS ADVERSE INFORMATION HAD BEEN REPORTED:

Excessive Financial Difficulties
 Daily viewing (several months) of television and news stories concerning espionage and defection
 Planned to buy three houses and a \$16,000 car

Report "Adverse Information" regarding cleared personnel to Security (see inside back cover).



**Drug Abuse & Security
 Don't Mix**

MARCH 1990

1	THURSDAY	
2	FRIDAY	
3	SATURDAY	
4	SUNDAY	
5	MONDAY	
6	TUESDAY	
7	WEDNESDAY	
8	THURSDAY	
9	FRIDAY	
10	SATURDAY	
11	SUNDAY	
12	MONDAY	
13	TUESDAY	
14	WEDNESDAY	
15	THURSDAY	
16	FRIDAY	

AMERICA'S

Thomas P. Cavanagh

MOST UNWANTED

EMPLOYMENT AT TIME OF ESPIONAGE:

Engineering Specialist, Northrop Corporation

CONVICTION DATE/SENTENCE:

May 1985 - Two concurrent life sentences

INFORMATION COMPROMISED:

None. Thomas was arrested by the FBI while attempting to sell classified U.S. documents from the Stealth Bomber project to the Soviets.

The FBI had received prior information of the event and subsequently developed a counterintelligence operation targeted against Thomas.

In reviewing the material that Thomas attempted to sell, defense experts concluded that had it reached the Soviets, U.S. National Security would have suffered severe damage.

MOTIVATION:

Money: Wanted to be "independently wealthy" Owed approximately \$41,000 to creditors (in addition to a \$98,000 mortgage)

Believed that his financial problems would prevent him from obtaining a Top Secret security clearance

ESPIONAGE THAT COULD HAVE

St. Patrick's Day

117
SATURDAY

118
SUNDAY

119
MONDAY

120
TUESDAY

121
WEDNESDAY

122
THURSDAY

123
FRIDAY

124
SATURDAY

125
SUNDAY

126
MONDAY

127
TUESDAY

128
WEDNESDAY

129
THURSDAY

130
FRIDAY

131
SATURDAY

BEEN STOPPED IF THIS ADVERSE INFORMATION HAD BEEN REPORTED:

Excessive Financial Difficulties
Job Dissatisfaction

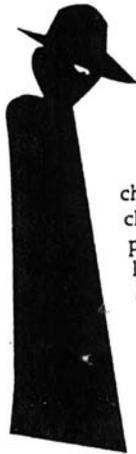
Report "Adverse Information" regarding cleared personnel to Security (see inside back cover).



National Security Is in Your Hands

The Counterintelligence Viewpoint

by Robert S. Vrooman,
Internal Security (ISEC) Officer



One of the most interesting effects of the democratic reform in Eastern Europe is the disposition of the various intelligence and security services. By no means are the changes uniform; no changes have taken place in the USSR. Poland, Czechoslovakia, and Bulgaria, on the other hand, have limited the power of the internal security services, but have not made any changes in the foreign espionage branches. Even though East Germany has disbanded the "Stasi" (State Security Service), Markus Wolf, one-time head of spy operations, has reportedly arranged to transfer human assets to the KGB. According to press reports, only Hungary has made changes that impact foreign espionage activities.

Remember

by Joanne Rader, OS-12

If you are planning travel to any of the DOE-listed sensitive countries, you must report it. If your travel is OFFICIAL, the reporting requirement is taken care of by completing Section 1a. of the "Request for Approval of Foreign Travel," DOE Form 1512.1 (call FIN-8, 667-2811 for the form). If your travel is UNOFFICIAL (vacation, etc.), you must complete DOE Form 1512.2 (call OS-12, 667-0077 for this form). The Department of Energy is required by law to brief

Poland, Czechoslovakia, and Hungary are also reported to have turned files over to the Soviets. However, it is questionable if the Soviets can pick up these assets since there are also many defections from the various intelligence services who are willing to trade information for political asylum in the West. To date, for example, five arrests have been made for espionage as a result of debriefing Stasi Colonel Alexander Schalck-Golodkowski. American intelligence officials have admitted to screening defectors for useful information. From October 1989 to January 1990, the Immigration and Naturalization Service statistics show that 376 persons from Warsaw Pact Countries were granted political asylum, while 341 were turned down. A percentage of those granted asylum were intelligence officers, according to the officials. Perhaps it is only a matter of time before there are some arrests in the U. S. as a result of the democratization of the Warsaw Pact.

all individuals traveling to sensitive countries prior to their departure whether the travel is OFFICIAL or UNOFFICIAL. Please call OS-12, 667-0077 for the written briefing material as well as information regarding the country(ies) to be visited. A video entitled "Before You Travel Abroad" is also available in OS-12 for your viewing. In the instance of OFFICIAL travel, submittal of DOE Form 1512.1 to FIN-8 must be made 60 days before traveler's departure. When travel is UNOFFICIAL, please submit DOE

Security System Bulletin

Operational Security &
Safeguards Division
Los Alamos National Laboratory
Vol. 5, No. 2, 2nd Quarter 1990

Charles A. "Robbie" Robertson -
Division Leader
Carl A. Ostenak - Program Director, SAO
Robert S. Vrooman - Officer, ISEC
Eugene Dashner - Program Manager,
OPSEC
Joanne Rader - Security System Bulletin-
Manager, B236, 667-0077
Ralph Montoya - Security Awareness
B236, 667-6901

Security System Mail Stops & Phone Numbers

OS-2, Material Control & Accountability,
E508, 667-5886
OS-4, Computer Security, G727, 665-1795
OS-6, Classification, F674, 667-5011
OS-8, Security & Safeguards Support,
G725, 667-4718
OS-10, Projects, Plans, & Policy, G728,
665-1212
OS-12, Personnel Security, B236, 667-5897
OS-14, Nuclear Material Transportation
& Storage, E587, 665-2715
OS Division Office, G729, 667-5911
SAO, Safeguards Assurance, G731,
665-2179
ISEC, Internal Security, G733, 665-2448
OPSEC, Operations Security, G728,
665-1212
COMSEC, Communications Security,
B270, 667-5113
EM, Emergency Management, K496
667-6211
Mason and Hanger, G724, 667-6534

LALP-90-1

Los Alamos National Laboratory, an affirmative action/
equal opportunity employer, is operated by the
University of California under contract W-7405-Eng-36
for the U.S. Department of Energy.

Form 1512.2 to OS-12 six weeks prior to departure. Who has the responsibility to report travel to sensitive countries? All individuals currently holding a "Q" Clearance or any one who has held a "Q" Clearance within the last five years.

Recommendations

After compiling the research results of this study, a number of themes presented themselves, from which we developed several recommendations. As can be seen in previous sections of this report, our research has shown an overall approval of the current Security Education and Awareness Program. Therefore, we will refer to the following as simply “enhancements.”

Organizational Identity

The development of a common logo is an effective way to represent the Security Awareness program to employees at all levels of involvement. A logo serves as a representative of security, visually portraying its underlying essence, while evoking the desired feelings of an outstanding security culture. Washington State University professors, Dr. Pamela W. Henderson and Joseph A. Cote, conducted a study to determine the characteristics of an effective logo; an article relating the results of this study was published on May 18, 1998 in the Wall Street Journal. Please refer to this article, which can be found in Appendix D, for guidelines to follow when developing your logo.

In addition to developing a logo, a complimentary slogan should be added as well, and should be consistent throughout all security communications.

When implementing these changes we recommend that you consider changing the name of the security awareness program to the "Security Involvement Program." Changing the name will send a message that a significant change is taking place. In addition, it will help focus attention on the true purpose of the program and serve as a reminder that security requires involvement not just awareness.

Implementation

Once developed, the Security Education and Awareness Program logo and slogan should not be changed. They should be present, highly visible, and consistent in size, location, and color in all media communications.

When implementing these changes, also consider changing the name of the security awareness program to the "Security Involvement Program." Changing the name will send a message that a significant change is taking place. In addition, it will help focus attention on the true purpose of the program and serve as a reminder that security requires involvement not just awareness.

Web Banners

Web banners should only randomly contain security messages in order to avoid the effects of what marketers call “adaptation theory,” or the tendency toward low involvement behaviors when dealing with repetitive stimuli. (Minor & Mowen, p.44) If

people can count on a security message in the same space on a routine basis, they will tend to naturally overlook that space on their screen. If the use of banner space is altered to a more unpredictable state, this can continue to be an effective means of communication.

Implementation

We are aware that the aforementioned banner space has been purchased by representatives of the Security Education and Awareness Program, and must be in constant use in order to maintain cost-effectiveness. Hence, we suggest varying the contents of the banners on a daily basis, with security messages appearing no more than twice per week. Other banner suggestions include:

Positive thoughts or quotes for the day

Example: “You can determine the quality of an individual by the standards they set for themselves.” -Anonymous

Home security tips

Example: Before going on a vacation, make sure to. . .

Stress-busters

Example: “Neck Stretch” – Imagine you have a pencil sticking straight out from your chin and sign your full name in the air as large as possible. (Stress Busters Calendar 2001, by Katherine Butler)

Trivia questions

Example: Who won the 1969 World Series?

Suggestion Box

This is an opportunity to welcome employee suggestions, thoughts, stories, or questions that relate to security, as well as ideas for future web banners or other media communications. There should be a system in place to give feedback to those people who participate.

*For a visual sampling of these ideas, see Appendix D.

Posters

When developing posters, ensure that the picture tells most of the story, with captions that are “to the point” and supportive of the picture’s message. Avoid negative, condescending, and/or threatening connotations at all times. Instead, focus on positive themes that link individuals to involving issues such as the importance of family and teamwork. Exercise caution when using humor, as studies have shown that if there are preexisting negative attitudes toward an idea, the use of humor may hinder the effectiveness of a related message. Always remember to include your Security Education and Awareness logo on all posters.

Implementation

We suggest that a professional marketer or communications specialist preview posters to ensure effective design, as well as to analyze any hidden themes. If this is not a feasible alternative, it is recommended that people outside the Security Education and Awareness Program be consulted for this purpose.

It is also recommended that limited funding be allocated to the creation of posters, as research showed them to be effective only when changed frequently. The funding this would require may be more effectively utilized in other ways.

Realism in Communication

Use real-life examples whenever possible to convey the importance of security. As mentioned in section 6, these examples do not have to directly relate to Hanford, but need only be relevant to the importance of security in the workplace.

As interpersonal communication was deemed highly effective by interviewees, it is important to create valuable face-to-face time. Most work teams schedule routine meetings to come together and discuss relevant information, however occasionally managers are left struggling to fill the time. We recommend developing “meeting scripts” that clearly outline a topic, update, story, or lesson for managers to follow during the meeting, and from which to derive group discussion ideas.

Implementation

A good example to follow as a general outline when developing a meeting script is a four-step process used by the Boy Scouts of America. This process is as follows:

1. Discuss what happened
 - a. Describe the who, what, when, where, and why?
 - b. Discuss any thoughts or feelings about what happened
2. Make a judgment
 - a. What did you like best/least?
 - b. What did you learn?
3. Generalize the experience
 - a. How does this activity relate to our work (at home or at work)
4. Set goals
 - a. What are we going to do about what we just learned?

*When following these steps, managers must not evaluate any employee responses, as this does not promote the sharing of ideas in the future. This is

simply a discussion tool that encourages free discussion. Managers may add their own “insights,” if there are particular points they feel a need to discuss.

Patrol Officers

As we’ve found, security patrol officers serve as a visual representation of the importance of security. They are perceived as the opposing side rather than co-workers. We suggest portraying patrol officers as members of the team working with employees toward a common goal.

Implementation

In general, implementation of this suggestion should involve depicting security patrol officers as individuals whose job entails protecting people and the work they do. Posters containing such images would be effective communication tools if used in areas where guards are present.

Specific Examples:

- A patrol officer and an office employee smiling together.
- Family surrounding a patrol officer who is holding a newborn child.
- Images of other situations in which people are protecting other people. See appendix D.
- Patrol officer sponsored events such as barbeques, food drives, etc.

Radio

We explored the possibility of implementing radio spots during the morning and afternoon commutes. This approach would involve either a radio talk show format, in which security issues are discussed on the air, or periodic placement of security ads. Although a creative idea, we do not recommend pursuing it at this time for the following reasons:

- Radio is typically a low involvement media
- The Hanford AM warning radio station is not an option due to a weak signal, high costs associated with strengthening the signal, as well as its primary usage as an emergency response radio station.
- Advertisements on local AM/FM radio stations would be very costly, as several ads would be required on different stations in order to reach a representative audience.

Partner with Safety

Partnering with the Safety program in communication efforts could prove to be very worthwhile. There are benefits to be gained from safety's established worker involvement levels by linking the ideas of safety and security together.

Implementation

Some elements of this recommendation may be easily implemented while others may take considerable time due to the need to coordinate and receive approval from DOE Headquarters. Although full integration may not be possible due to the special needs of security programs, there are a many activities that may provide near-term results at Hanford. These actions require considerable effort in the development and early implementation phases.

Potential Hanford actions include:

- Consultants have the advantages of being neutral parties as well as being able to focus their efforts on a single task. Consider using outside consultants to help design and support integration of the more complex actions identified below.
- Share the web-banner space with safety and health. This valuable tool can augment the safety program communications channels and be a gesture of good will.
- Establish a liaison with VPP that will allow sharing of the interpersonal communication channels used in VPP.
- Consult with VPP and Enhanced Work Planning managers within Fluor Daniel Hanford to identify potential areas where security and safety programs can share communication channels and other resources. (There are national networks established within these two programs that can be used to help identify successful strategies and approaches.)
- Network through and use the experience of the Hanford Patrol members, whom are actively working on site safety committees, to identify new areas of common opportunity and best approaches for building employee security involvement at Hanford.
- Consult and partner with the Hanford Labor Unions to build support for security awareness as an employee driven program.
- Team-up with safety on posters, as well as co-sponsoring employee events, such as barbecues or awareness weeks.

Potential DOE level actions include:

- Develop a proposal to be a "security involvement pilot program" site. As a pilot there exists an opportunity to develop a method to successfully integrate the functions of the security awareness program with safety and health. This approach can increase available resources for a short period of time, raise the visibility for the actions being taken, and provide an opportunity to experiment with innovative approaches. The success of VPP at Hanford and existing support from the Labor Unions make Hanford an excellent location for creating and demonstrating new approaches.
- Use the Security Education Special Interest Group as a conduit to other DOE sites to build support and recognition for the value of working cooperatively with safety programs.

Increase Employee Involvement

Identify involvement opportunities that increase contact, interactions, and joint development activities with employees and managers. Empower employees to influence the programs and decision-making processes that impact their work environment.

Implementation

The approach taken in the security awareness program can be enhanced through implementation of VPP-like employee and manager involvement activities.

- Make a conscious effort to increase the time spent listening to Hanford managers and workers.
- Develop processes and activities that encourage and support employee involvement.
- Increase involvement in security awareness matters by creating an interpersonal communications channel.
- Identify manager and employee behaviors that demonstrate acceptance of safety culture values.
- Encourage managers to use behaviors that increase employee involvement, ownership and commitment. Employees can help define these characteristics by answering the following three questions:
 - What management behaviors and characteristics influence you to have the highest levels of involvement, ownership and commitment?
 - How is management performing with respect to these behaviors and characteristics?

- What management actions can have the greatest immediate impact on improving your level of commitment?
- Communicate to the workforce, your customers and clients, that this improvement effort takes time to become fully integrated into the work environment.
- Use site and local resources to help PTH develop successful involvement strategies. These resources can also provide consulting services to help plan and implement organizational changes.

Measure Behaviors, Attitudes and Beliefs

Define and implement new performance indicators that measure behaviors, attitudes and beliefs that are important to security and the security awareness program.

PTH has expressed the desire to achieve increased levels of involvement and ownership for security awareness. The adage that "what gets measured gets done" supports the notion that behaviors, attitudes and beliefs about security awareness should be measured.

Implementation

- Use the Hanford VPP survey to measure site security involvement.

The Hanford VPP survey conducted in 1999 provides an approach that could be used with minor modification to measure VPP-like behaviors that are needed to enhance security involvement at Hanford. The survey consists of fifteen elements and is administered by Fluor Daniel Hanford (FDH). The survey was constructed to measure three behaviors that support each of the five VPP tenets. There are many elements of this survey that may directly measure, or could be modified slightly to measure, desired security awareness behaviors. Appendix C provides a copy of the Hanford VPP survey questions and an analysis of the 1999 survey results.

- Benchmark security awareness performance using VPP criteria.

There is an opportunity for further research into security awareness, involvement, and ownership at Hanford by comparing VPP and Security Awareness programs using the VPP survey results as a benchmark. The security awareness survey conducted during this study demonstrates that security messages are being communicated to the workforce; however, the survey was not designed to measure involvement, ownership or commitment.

- Implement measures of manager and employee attitudes, values, and beliefs that are consistent with an outstanding security culture.

Although the VPP program measures behaviors, it does not measure attitude and

beliefs. The security experts consulted in this study provided insights into the attitudes and beliefs that they indicated would be part of an outstanding security awareness culture. A more comprehensive list of attitudes and beliefs could be identified using a process like the one used in developing the sample security culture performance measure in this study. Once standards of beliefs and attitudes are developed, these attributes can be incorporated into a more traditional survey process.

- Use site and local resources to help PTH develop successful involvement strategies. These resources can also provide consulting services to help plan and implement organizational changes.
- It may be desirable to use consultants in implementing this recommendation.

Two potential individuals to contact at Hanford are Jim Schildknecht of the FDH Program Support Department (process and approach) and Steve Prevette in FDH ES&H Department. Jim Schildknecht has served as chairman for a DOE-wide Enhanced Work Planning working-group and recently lead a very successful DOE Annual Integrated Safety Management Conference hosted by Hanford. Steve Prevette is a nationally recognized expert in statistical process control and can assist in the development of behavioral measures.

- Communicate the results, as appropriate, to management and the workforce.

Graded Approach for Communicating Security Information

There is an opportunity to improve relationships between Security and the workforce by developing a process to communicate and resolve the conflicts that exist between security's need for secrecy and employees' needs to understand why security requirements are needed.

Implementation

- Form an advisory group (comprised of security specialists and a diverse Hanford employees with security clearances) to identify the types of information needed by employees to understand why security requirements are important and to keep their awareness and ownership strong.
- Develop and institutionalize a process that will serve the needs of both secrecy and employee security awareness motivation.
- Pilot the process at one of the Hanford facilities to improve the final product and to build grass roots ownership and support for the new process.
- Develop a site-wide implementation strategy that:

- Allows for tailoring of processes at each facility
- Involves employees and managers
- Communicates why secrecy must be maintained for some aspects of security
- Measures to verify that adequate levels of communication with the workforce are being achieved

Staffing

As managing the SEAP is an enormous responsibility, and communicating to the employees on a routine basis is difficult for a single person to do, we recommend additional staffing for this program. We are aware that resources are very limited, so we are offering an alternative to simply hiring new employees. There are many resources available in the Tri-Cities that could benefit the SEAP. One such resource is the Washington State University, Tri-Cities undergraduate and graduate intern program. There are many talented students attending this school who are looking for jobs during the semester that allow them to be flexible around class schedules. This way, the SEAP has some “fresh” talent when they need it most, and students earn some money and receive a valuable learning experience, while earning college credit. As has been demonstrated during the course of this study, this is a win-win situation.

Implementation

Contact the Business Links office at WSU Tri-cities for more information about this program and the availability of business or marketing interns.

Security “ED”

Our final recommendation relates to the Security “Ed” cartoon currently being used at Hanford. We analyzed samples for any possible enhancements, and came up with a few recommendations. First, Ed may need to “get out of his recliner” and get involved with the situations taking place in the cartoon. Additionally, in order to get the workforce more involved, we suggest awarding a prize to anyone who submits an “Ed” idea that is implemented. Ask employees to come up with captions, locations for Ed to travel to, or situations to be depicted, and reward those who have the most creative ideas. Another suggestion is to make sure the messages are positive, and free from condescending undertones, which may require some further analysis upon development of a cartoon. Refer to the Content Analysis section of the report for a more detailed examination of condescending language in communications.

As “Ed” was frequently confused during interviews as “security education,” it may be necessary to consider renaming him, or making him easily recognizable in some other way. Finally, we recommend that if the mouse is a pivotal character, and should not be removed from the cartoon, it needs to move around and be more involved in the events

that are occurring. It also does not necessarily have to comment in every situation. Table 7.1 summarizes our analysis of Security “Ed.”

Table 7.1

STRENGTHS	WEAKNESSES
<ul style="list-style-type: none"> ➤ Short, focused messages are more likely to reach people at lower levels of involvement ➤ “Ed” is versatile, allowing many different people to relate to him ➤ When done effectively, a cartoon can be a good way to get people’s attention ➤ Templates are inexpensive and easily adaptable ➤ It is good for the SEAP to have a “spokesperson,” as Ed appears to be ➤ “Ed” received a warm response at the TRADE conference in DC, generating much excitement among security awareness coordinators from around the country; a national security spokesperson wouldn’t be a bad idea. . . . 	<ul style="list-style-type: none"> ➤ Those cartoons with too much dialog, or too many sources, can prevent the message from being absorbed; the mouse seems to complicate the source in that it is simply restating (in different words) what has already been said ➤ The mouse appears to represent the employees, as it is looking at the reader of the cartoon, and seems to be addressing them; this linkage between a mouse and an employee who feels like “the little guy” could be counterproductive ➤ Low involvement people may interpret the image of a recliner as a symbol of laziness; linking this idea to security will not encourage active participation ➤ Templates may be too restrictive, as positioning of characters and objects within the cartoon does not change; the concept of novelty, or people’s need for change, applies here; lack of change could lead to a loss of appeal ➤ Security is portrayed at a distance, as “Ed” is always outside of the situations he is commenting on; could project feelings that employees are “being watched” by security, as if they aren’t trustworthy; this also does not promote security as a real part of everyday life, as the SEAP wants it to be; dictatorial image

Implementation

Ideas for implementation of this alternative include a “Where’s Ed Now?” campaign in which “Ed” keeps popping up in strange places and encounters situations relating to different types of security (example: “Ed Goes Fishing,” “Ed Goes on an Overseas Business Trip,” “Ed in the Jungle”). This would be a way for “Ed” to get out of his chair, and keep the employees guessing. If his identity is to continue to be unknown, this could be done very creatively in each situation (refer to “Home Improvement” television show’s “Wilson” character). This idea would fit well with having employees submit ideas for the cartoon. Ask them to submit ideas as to where Ed should go next, and what kind of situation he’ll find himself in.

Actions

Action Items

- Develop of a common logo and slogan
- Web banners should randomly contain security messages
- Poster graphics should tell the story and use to-the-point captions
- Portray patrol officers as members of the team working with employees
- Partner with the safety program
- Identify employee involvement opportunities
- Define and implement new performance indicators
- Resolve conflicts between security's need for secrecy and employees' needs to understand why security requirements are in place
- Additional staffing for the program
- Get Security "ED" more involved

Appendix A

Expert Insight into the Characteristics of a Security Awareness Culture

A sample performance indicator that describes and evaluates DOE security awareness culture was created using the results of five structured interviews. These results are not valid because of the sample size but they are interesting, potentially useful, and demonstrate a method to measure "fuzzy" concepts such as culture, ownership, involvement, or satisfaction.

Methodology

Five senior managers with expert security backgrounds were interviewed using open-ended questions. Three of the managers are located at DOE Headquarters while the other two are at the Hanford site.

The security experts were asked, "to describe the characteristics of an outstanding security awareness culture." In each case the experts identified multiple characteristics. They were next asked to group similar thoughts and then define the new grouping of ideas. The phrase they used to describe a grouping of similar ideas is referred to as a "characteristic."

The expert was told to distribute one hundred points between all of the identified characteristics based on its relative importance. During this evaluation the expert discussed the reasoning for arriving at the assigned priority. In each step of the process the reasons and comments were documented in the notes.

Next the safety expert was asked to "evaluate the current performance of each characteristic on a scale from one to ten." For this evaluation task a zero represents a condition where "it isn't happening at all," and a ten equates to, "it's perfect." (This evaluation step was done in four of the five interviews.)

In the last step of the process, the security expert was asked, "If there were only a few things you could do to achieve the greatest improvement in this performance indicator, what would they be?"

To generate the composite indicator, similar characteristics were combined to form blended characteristics. A simple averaging technique was used to determine the values because a statistical approach would not be appropriate with five interviews.

The following italicized statement is derived from the interview notes. It provides blended, but not validated, vision of the security awareness culture that these experts are trying to achieve.

"A security awareness culture has ownership for security principles. Individuals value security and understand why security is important to them. Managers are actively involved in delivering the security message. They demonstrate the importance of security through their actions, and they have a clear communication path between themselves and their employees.

Programs deliver effective and relevant messages that are easily understood, accepted

and delivered by managers to the workforce. The performance of the program is routinely evaluated to ensure it is achieving its goals of awareness and ownership.”

(A1-A7, Personal communication, March, 2001).

Table 1 contains quotes describing the "characteristics" identified by the security experts. The first level of bullets represents the characteristic.

Table of Characteristics Identified

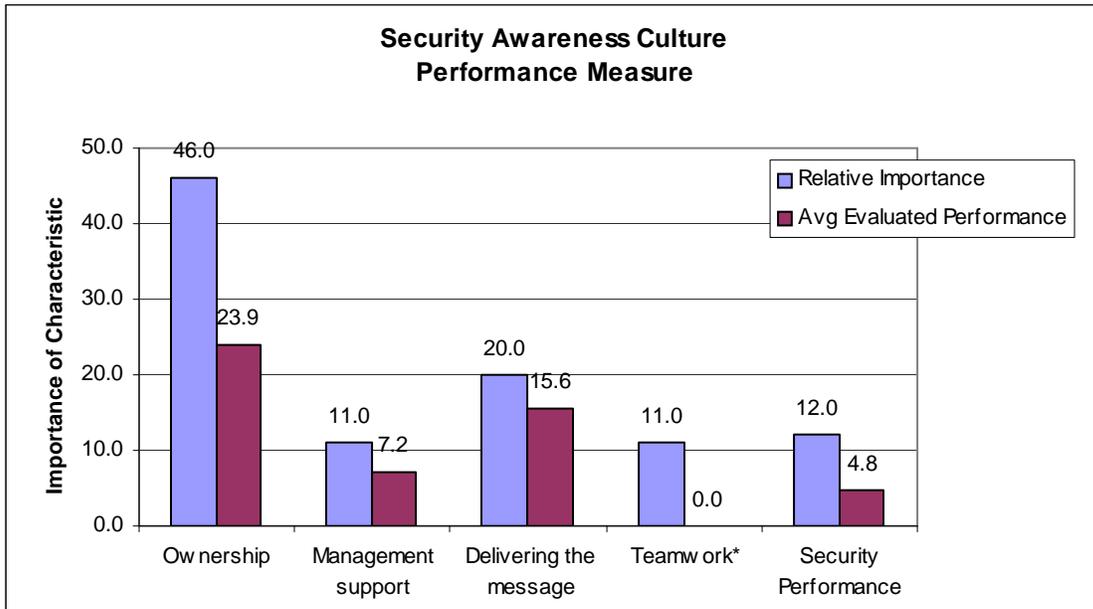
Composite Term	<i>The underlying values, beliefs, and behaviors</i>
"Ownership"	<ul style="list-style-type: none"> • <i>There is personal ownership for security</i> • <i>People have a higher sense of appreciation for security</i> • <i>People value security (2 individuals)</i> • <i>Security is integrated, it's a routine way of doing business</i> • <i>People do security</i>
"Management Support"	<ul style="list-style-type: none"> • <i>Managers support the security awareness program</i> • <i>There is organizational commitment to security</i> • <i>Managers are involved</i>
"Delivering the Message"	<ul style="list-style-type: none"> • <i>The content of security awareness training is comprehensive</i> • <i>The security awareness creates an enhanced learning experience</i> • <i>The security awareness message is effectively delivered</i> • <i>Security Coordinators are effective</i> • <i>The security awareness message has impact</i>
"Teamwork"	<ul style="list-style-type: none"> • <i>There is teaming in the development and implementation of security</i> <ul style="list-style-type: none"> ○ <i>The security team is part of the security culture.</i> ○ <i>"It's not us versus them," it's, "we're in this together."</i> ○ <i>There is collaboration on how to implement security effectively.</i> ○ <i>There's an attitude in the Security department that "we're here to help you meet mutual objectives."</i> ○ <i>Your success is important to my success</i>
"Security Performance"	<ul style="list-style-type: none"> • <i>We have security results</i> <ul style="list-style-type: none"> ○ <i>People put the security of the facility above potentially hurting the feelings of the people around them.</i> ○ <i>We are safeguarding special nuclear materials.</i> • <i>There is performance feedback:</i> <ul style="list-style-type: none"> ○ <i>There are well-established feedback mechanisms.</i> ○ <i>1) How are we doing?</i> ○ <i>2) How do we know?</i> ○ <i>Problems are identified corrected immediately.</i> ○ <i>There are few or no security infractions or violations.</i>

In two of the groups a second level of bullets was added to clarify the characteristic. There are a total of 16 characteristics that were combined to create the composite indicator shown

below.

Figure 1 is a sample security awareness culture performance indicator. The column on the left in each characteristic represents the relative importance out of a total of one hundred possible points for the entire indicator. The column on the right is the perceived level of current performance on the characteristic.

Figure 1



Sixty-eight percent of the total available points for this performance measure were assigned to elements associated with an individual's role and the importance of interpersonal relationships. In particular, there is clear consensus among these senior managers that ownership can have a substantial impact on the security awareness culture and presents an excellent opportunity for improvement.

A.1

Marketing Analysis and Strategy Formulation for Project Hanford Security Education and Awareness Program			
Interviewee:	Company: PTH	Title:	Segment: Senior Manager
Phone #	Loc:	Time @ Hanford:	Email:
Interviewer: Alison Marcum	Date of Interview: 3-30-01		
Interview Summary			
Highlights of Interview			
Question T1:	What are the elements of an outstanding security culture?		
Reply: Element 1	Awareness and Ownership: An "I take personal responsibility" attitude; people confront strangers; knowledge isn't enough-attitude makes the difference; management setting an example shows that management takes ownership of security		
Reply: Element 2	Teamwork: "We are in this together" attitude rather than Us vs. Them		
Reply: Element 3	Measurement: is tangible; must allow management to see if things are working		
Question T1a:	How important are each of these elements? Why?		
Reply: Element 1	50% - no further explanation (See A.2 interview, as they were in agreement on this)		
Reply: Element 2	30% - no further explanation (See A.2 interview, as they were in agreement on this)		
Reply: Element 3	20% - no further explanation (See A.2 interview, as they were in agreement on this)		
Question T1b:	On a scale of 1-10, 1 being low and 10 being outstanding, how would you rate each element? Why?		
Reply: Element 1	3 – based on his perceptions of and interactions with employees; incident trends (violations, feedback); security is viewed as a compliance issue rather than an "It's important to me" issue; people think of it in terms of infraction notices received for noncompliance		
Reply: Element 2	4 – there are pressures associated with some missions-security is seen as dispensable and is one of the first things to go out the window when pressures are up		
Reply: Element 3	5 – due to lack of resources (budget, work requirements, productivity requirements) – an "I'll devote the minimum amount of time that I can get away with" attitude; what causes managers to put so much more emphasis on safety than security?		
Question T2:	If there were one or two things that could be done to increase employee ownership of security, what would they be?		
Reply:	Sponsorship of security (VPP program should include safety and security together)		

A.2

Marketing Analysis and Strategy Formulation for Project Hanford Security Education and Awareness Program			
Interviewee:	Company: FH	Title:	Segment: Contr Mid.Lvl.Mgmt
Phone #	Loc:	Time @ Hanford:	Email:
Interviewer: Alison Marcum	Date of Interview: 3-30-01		
Interview Summary			
Highlights of Interview			
Question T1:	What are the elements of an outstanding security culture?		
Reply: Element 1	Awareness and Ownership: An "I take personal responsibility" attitude; people confront strangers; knowledge isn't enough-attitude makes the difference; management setting an example shows that management takes ownership of security		
Reply: Element 2	Teamwork: "We are in this together" attitude rather than Us vs. Them		
Reply: Element 3	Measurement: is tangible; must allow management to see if things are working		
Question T1a:	How important are each of these elements? Why?		
Reply: Element 1	50% - Example given: What causes a person to follow the speed limit? What causes a person to go 65 instead of 55? They know the speed limit, but something causes them to choose one alternative over another. (It's the basis of the decision that matters here-the "why" aspect)		
Reply: Element 2	30% - Having employees be part of a team allows for better reception of security responsibilities; managers can provide quality training materials so they know the rules, but it is then their responsibility to run with it		
Reply: Element 3	20% - In order to obtain funding, measurement of whether or not the job is being done is extremely important-(doesn't necessarily drive ownership and teamwork, however)		
Question T1b:	On a scale of 1-10, 1 being low and 10 being outstanding, how would you rate each element? Why?		
Reply: Element 1	7 – based on the large population at Hanford compared with the number and type of incidents-incidents are low compared to population; security incidents that do occur are usually common things that are not considered huge infractions; when there are critical infractions, it is usually a result of one individual not doing what they're supposed to rather than an entire group of people		
Reply: Element 2	3 – he does see an "Us vs. Them" attitude; it was a real eye-opener to him when he handed out 400 giveaway items one day and people reacted surprisingly (Example: "You're giving me a gift? You usually only tell us when we do things wrong."); he thinks people see him and security as the enforcer		
Reply: Element 3	4 – Managers are doing what is expected, but are not going above and beyond-there is no consequence from contractors in order to motivate them to put forth more energy; in need of senior manager support-not a solid foundation if not there; safety program has monetary consequences attached to it as well as contract accountability-security does not have these consequences in place		
Question T2:	If there were one or two things that could be done to increase employee ownership of security, what would they be?		
Reply:	Sponsorship of security – VPP (which now focuses solely on safety) should include security as well		

A.3

Marketing Analysis and Strategy Formulation for Project Hanford Security Education and Awareness Program			
Interviewee:	Company: Battelle	Title:	Segment: Senior Manager
Phone #	Loc: PNNL	Time @ Hanford:	Email:
Interviewer Dennis Walters	Date of Interview: 3/21//01		Sent
Question T1:	What elements create an outstanding security awareness and ownership culture?		
Reply: Element 1	There is personal ownership for security: Security is perceived as a value, not an impediment. Individuals feel ownership for security.		
Element 2	There is organizational commitment to security: There is upper management support and commitment to security. They actively support and set the example for the workforce.		
Element 3	There is teaming in the development and implementation of security: The security team is part of the security culture. "it's not us versus them" it's "we're in this together." There is collaboration on how to implement security effectively. There's an attitude in the Security department that "we're here to help you meet mutual objectives." "Your success is important to my success."		
Question T1a:	How important are each of these elements? Why?		
Reply: Element 1	30 - This is the outcome		
Element 2	15 - This is the enabler		
Element 3	55 - This is how we get there		
Question T2:	If there were one or two things that could be done to increase employee ownership of security, what would they be?		
Reply:	<ul style="list-style-type: none"> - People need to understand why we are doing security, what we are trying to achieve. This is a challenge because in many cases we cannot disclose the specific nature of the threat because the reason is classified. - We need to develop trust for the government so workforce will do accept security requirements even though they don't understand all the reasons. Element 2 can help this by making it clear they endorse the security measures (people are more willing to trust people than the government) When the message is coming from management it is not coming from the government. - Particularly at the Laboratory, people always want to know why. The spend most of their lives answering the question as part of their research. 		
Observations:	<ul style="list-style-type: none"> - People don't think in terms of economic and business threats. - Communications is the key to doing each of the elements. 		

A.4

Marketing Analysis and Strategy Formulation for Project Hanford Security Education and Awareness Program			
Interviewee:	Company: Wackenhut Services	Title:	Segment: Senior Manager
Phone #	Loc: NNSI, DOE	Time @ Hanford:	Email:
Interviewer Dennis Walters	Date of Interview: 3/26/01		Reviewed
Question T1:	What are the attributes of an outstanding security culture?		
Reply: Element 1	<p>People have a higher sense of appreciation for security: –Security awareness training must be relevant in that it clearly communicates to the individual: "how do the requirements apply to me." The information is concrete and meaningful. Individuals consider security awareness to be an integral part of their work toward protecting themselves and information. Like a safety program, security awareness is fully integrated into employees' daily actions; not a separate or remote action. The culture embraces security and regards it as a valuable part of the job, not a necessary evil.</p>		
Element 2	<p>The content of security awareness training is comprehensive: The security briefings cover all of the information people need to know to implement security effectively.</p>		
Elements 3	<p>The security awareness creates an enhanced learning experience: Briefings are fun and interesting. The participants find it enlightening, engaging, interactive, and challenging; all of which increases awareness. The briefings try new things to be more successful at engaging the workers.</p>		
Question T1a:	How important are each of these elements? Why?		
Reply: Element 1	60 % - No matter what you have for content, you need motivated people to achieve an outstanding security culture.		
Element 2	10 % - It needs to be comprehensive. The information is well defined. Since we have the content, the other two elements are more important.		
Elements 3	30% - The delivery of the message is important to achieving the motivation we desire.		
Question T1b:	On a scale of 1-10, 1 being low and 10 being outstanding, How would you rate each element? Why?		
Reply: Element 1	6 - The people I've come across in the security awareness-training field have acknowledged the importance of security. They are able to tell people what needs to be done to meet security requirements but are struggling with how to best motivate the workforce. We know what we want to do but we don't know how to do it.		
Element 2	9 - The information that needs to be communicated is well defined and well known.		
Elements 3	7 - We know there are many different mechanisms available to use. We have many different media and approaches available. We need to enhance our use of the media that is available. For instance, being able to create a video that has impact.		
Observation:	- Internal motivation is the key to success in developing the security culture.		
Question T3:	If there were one or two things that could be done to increase employee ownership of security, what would they be?		
Reply:	<ul style="list-style-type: none"> - Relevancy is the most important message we can send. They need to know, "how this is important to me" - We need to increase the perception of how important each person is to achieving security. There is a difference between authority and power. Individuals may not be in a position of great authority yet they may exert great power. For instance, a filing clerk has great power in protecting information security even though the position may not have mission authority. - Enhance each person's understanding of how incredibly important they are in protecting security. They should come away with the feeling, "Wow! I didn't realize how important I am. I'm really important here!" - There needs to be some means of telling particularly the scientific community at large that equal to their intelligence that is important to DOE, their awareness and appreciation for good security practices is also of great value. To instill in the individual their "worth." - People should come away from briefings with an understanding that they are "high up there" in the security scheme of things. 		

A.5

Marketing Analysis and Strategy Formulation for Project Hanford Security Education and Awareness Program			
Interviewee:	Company: Protection Technology Hanford	Title:	Segment: Senior Manager
Phone #	Loc: Hanford	Time @ Hanford:	Email:
Interviewer Dennis Walters	Date of Interview: 3/21//01		reviewed
Question T1:	What are the attributes of an outstanding security culture?		
Reply: Element 1	We have security results: People put the security of the facility above potentially hurting the feelings of the people around them. We are safeguarding special nuclear materials		
Element 2	People value security: Every person is dependable and reliable. There are consequences for being security conscious and for not being security conscious. Individuals find it is more rewarding to be security conscious. There is a perceived value to doing security right. (People are aware of how important security is at PFP for instance.) The level of security is graduated to meet the level of potential threats. Security people are doing something worthwhile. They are viewed as being assets.		
Elements 3	Security in integrated, it's routine way of doing business: It's a state of mind, people don't have to be reminded. They don't have to think about it. It's a work habit. People believe "security makes me safer in my job. It helps be get my job done. It's part of doing a good job." Workers are observant and know what's going on around them. They are aware of the people around them. "We are doing our part to ensure that unsavory people don't get access, whether they are employees or not." Security is looked at in a positive way.		
Question T1a:	How important are each of these elements? Why?		
Reply: Element 1	40 % - We must have security results or the program is not achieving what it is intended achieve		
Element 2	10 % - Recognizing personal benefit is a byproduct of creating a security culture. When the culture is in place and security is being achieved, people will perceive the benefits of security. This element is highly dependent on the performance of the other two.		
Elements 3	50% - We must have the culture to be successful, once we get that we're half done. When we have the culture results will happen.		
Question T1b:	On a scale of 1-10, 1 being low and 10 being outstanding, How would you rate each element? Why?		
Reply: Element 1	Not evaluated or discussed.		
Element 2	<p>2 - because people don't think of security as a benefit at all.</p> <ul style="list-style-type: none"> - People probably do not see security as a benefit. The see it as a necessary nuisance. - There are trade-offs that tend to favor "security is a nuisance versus it's a benefit." - Security is not perceived as a strong negative, but it's not perceived to be a benefit either. 		
Elements 3	<p>6 - We have the admin challenges, were a security person enters a work site without properly displaying his badge. People are taking responsibility for security as evidenced by their challenging the person who does not display his badge.</p> <ul style="list-style-type: none"> - When people see what they consider to be a security infraction they are acting on it. - Managers are responding favorably to security assessment results. - There is increasing emphasis on security. The manager at PFP is allowing security to use the entire content of the facility newsletter for security messages. - For the most part, people are aware of where they work and know that they need security - Security representatives have good relationships with the building emergency directors - People inquire about security requirements when they are confronted with something they are not familiar with. - We are providing positive rewards through "Security Pays in Many Ways" - There are visible signs the people are following security requirements, - There is still room for improvement 		
Observations:	<p>As the importance for what we are guarding has gone down, people's irritation with security have gone up.</p> <ul style="list-style-type: none"> - The risk perceived by the worker is less than the risk perceived by security. They don't understand what is at stake. 		
Question T3:	If there were one or two things that could be done to increase employee ownership of security, what would they be?		
Reply:	<p>I think there needs to a consequence for behavior. If there aren't consequences, people won't change. People need incentives before they will change their perceptions and behavior. Security Pays... and the Admin challenge (limited scope performance tests) provide positive incentives, there do not appear to be any negative incentives, but some are needed.</p> <ul style="list-style-type: none"> - Advertising can have a tremendous impact on people. It can help change people's behaviors. - We use posters, but they are of limited use because they are no longer perceived after a couple of days. I can still remember the tuneful jingles from years ago, and TV ads like, "where's the beef." We need more innovative ways of sending the message. - People spend about an hour/day commuting. Perhaps we should be using radio ads, or audio tapes, or 		

	<p>CD's</p> <ul style="list-style-type: none">- With products you get immediate gratification, products cost money- There is little gratification for being secure. It doesn't cost money.- Only when security fails do we realize the need.
--	--

A.6

Marketing Analysis and Strategy Formulation for Project Hanford Security Education and Awareness Program			
Interviewee:	Company: DOE - HQ	Title:	Segment: Senior Manager
Phone #	Loc:	Time @ Hanford:	Email:
Interviewer Dennis Walters	Date of Interview: 3/30//01		Reviewed
Question T1:	What are the attributes of an outstanding security culture?		
Reply: Element 1	<p>People do security: Personal responsibility and Ownership: There is extremely high individual responsibility and ownership. Security is in individual's own responsibility. People believe and have a strong internal sense of how important security is to them. "It's not people sitting in some remote ivory tower, If my responsibility, not somebody else's." <u>People are encouraged and supported</u> in identifying problems and raising issues. If there is a problem it's identified and corrected immediately. Doing security is second nature. <u>We do it without thinking.</u> It's a habit. It's like wearing a TLD (Thermo-luminescent device). We don't have to think about it. <u>People are alert</u> to problems around them. They are observant. <u>Security transcends the work place</u> into the employee homes and personal lives. People see the value and benefit of security. They take it home with them.</p>		
Reply: Element 2	<p>Managers are involved: Integrated security culture. The security culture integrates into and supports the site's mission and objectives. It's viewed as supportive. <u>Everyone knows what is required.</u> There are clear roles and responsibilities. Senior management is actively involved in the security program. Their messages are consistent and frequent. They demonstrate personal commitment. They want to be treated the same when it comes to meeting security requirements and following security processes. There are no special exemptions because they are managers. They set the example. The managers use a well-established feedback process that answers the questions: 1) How are we doing? 2) How do we know? Problems are identified corrected immediately.</p>		
Reply: Element 3	<p>There is performance feedback: There are well-established feedback mechanisms. 1) How are we doing? 2) How do we know? Problems are identified corrected immediately. There are few or no security infractions or violations.</p>		
Question T1a:	How important are each of these elements? Why?		
Reply: Element 1	60 % - the culture is the people. It's how they think. It's how they work. It's how they do security. It's their attitudes. It's the most important part. It's the grass roots of an outstanding security culture.		
Element 2	20 % - Managers can command or demand, but they can't make it happen. They can set expectations. Share visions of what they would like to achieve. They can describe the culture they are trying to achieve. But unless the people buy into it, it is clear, and it's unambiguous, management wont achieve their security goals.		
Element 3	20% - It's at least as equally important as the manager's role because unless we can measure and answer the questions we don't accomplish anything. How do we know that people have bought into the culture? We need a process to measure the things that we can measure. There's an old adage, "you can't manage what you can't measure." This is true.		
Question T1b:	On a scale of 1-10, 1 being low and 10 being outstanding, How would you rate each element? Why?		
Reply: Element 1	6 - If you look at this element in total across the complex, people don't seem to understand how important they are to security at the site. People don't really understand the value of security. They don't know why we have do security. Or why we do it a certain way. They don't know what the threat is. People do not generally feel compelled to identify or report security problems. The Department has had a lot of changes in security management. This turnover has resulted in many different approaches. People seem to think, "This is the latest and greatest thing...in another six month to a year it will be something else. Why get too excited about it." There is no continuity or stability in the security program. Our security policy, as it exists today is ambiguous and can be interpreted in a variety of ways. It is subject to interpretation. New people can choose what it means.		
Element 2	6 - We just started doing some upfront work on creating an integrated safeguards and security management approach, but that's only in some parts of the department. The line organizations only see the lower left hand corner of the big picture. I would rate this lower but occasionally we run into some security operations where there are managers who know what security is and what it needs to be integrated. But very few have the program in place. Managers have given interviews in local newspapers saying that security requirements are expensive, of little value and have been delaying project work. "how do you think the workforce feels about security in light of comment like this?"		
Element 3	4 - The security awareness program is meant to be a "briefing" program not a "training" program. Consequently, there are no certification or qualification tests. It may be the next logical step to require testing if there is no other way to determine levels of awareness. The problem is how to measure awareness? In the current program the information flow all goes outward. We measure the quality of the delivery through feedback processes but we do not measure the level of awareness being achieved.		
Question T3:	If there were one or two things that could be done to increase employee ownership of security, what would		

	they be?
Reply:	- The feedback mechanism needs to be improved. We need to know, how are we doing and how do we know?

A.7

Marketing Analysis and Strategy Formulation for Project Hanford Security Education and Awareness Program			
Interviewee:	Company: DOE - HQ	Title:	Segment: Senior Manager
Phone #	Loc:	Time @ Hanford:	Email:
Interviewer Dennis Walters	Date of Interview: 3/27//01		Reviewed
Question T1:	What are the attributes of an outstanding security culture?		
Reply: Element 1	Individuals value security awareness: People are aware that security is a good thing. They value it and take it seriously		
Reply: Element 2	Managers support security awareness program: There is full participation and sponsorship from the top of the organization. The money and resources are adequate to ensure security. The program gets the attention it deserves. Management encourages participation in security activities include the Security Education Special Interest Group.		
Reply: Element 3	The security awareness message is effectively delivered: There is consistency in the implementation of security awareness policies. People are receiving briefings that are similar in content, how they are delivered, and when they are done. The information provided is uniform across the complex.		
Element 4	Security Coordinators are effective: Coordinators have responsibility for delivering the briefings. There is low turnover rate.		
Element 5	The security awareness message has impact: New approaches are used to communicate the security awareness message to keep the information fresh. There are sufficient funds for providing promotional materials like brochures and trinkets. People come out of the briefings with an appreciation for security and their responsibilities.		
Question T1a:	How important are each of these elements? Why?		
Reply: Element 1	20 % - The individual has to know the "why's and how's." They know that they are issued their badges for a reason. The know security is for their own protection. They accept their personal responsibility.		
Element 2	20 % -The security coordinator depends on his management to support the conduct of his activities. They need management backing to take the risk of trying new approaches to communicating security awareness to the workforce. If there are infractions the manager is held accountable so it's important that he trust the security coordinator to do a good job.		
Element 3	15% - The right message needs to get out: 1) Awareness of site specific needs, 2) Required material, and 3) It needs to be shown how it is relevant		
Element 4	30% - The new employee's first encounter with security education is with the security coordinators. This first impression is essential. The coordinators also need to be a resource that is approachable and readily available to the employees.		
Element 5	15% - This is where it comes together. The workforce knows how to be successful as they do their work.		
Question T1b:	On a scale of 1-10, 1 being low and 10 being outstanding, How would you rate each element? Why?		
Reply: Element 1	6 - My experience is that people don't take security awareness seriously enough. At a place like Pantex it's obvious but at many DOE locations security awareness isn't seen as relevant. They don't see the risk. However, many do take security seriously, I believe more than half do understand how and why security is important to them.		
Element 2	7 - There are many managers that do what they can but funds and resources are still short.		
Element 3	8 - Excellent message. New comers to the security awareness have the SE-SIG networking resources to help them.		
Element 4	8 - Most of the people I deal with are doing the best they can. They are experienced and are able to deliver the message. They are committed to achieving a high degree of security awareness.		
Element 5	7 - There are still some incidents and infractions. At the 10 level there would be no infractions.		
Observations:	- Security at DOE has improved over the past 2 years. The General has helped increase security awareness. Last year he spoke at the SE-SIG, we were energized at the SIG. (When there are expensive speakers or timely/pertinent presentations at a DOE site, it would be good to simulcast the event and video tape it for use at other sites)		
Question T3:	If there were one or two things that could be done to increase employee ownership of security, what would they be?		
Reply:	- Resources and money are needed to really improve security awareness.		

A.8

Marketing Analysis and Strategy Formulation for Project Hanford Security Education and Awareness Program			
Interviewee:	Company: Honewell (FMNT)	Title: Int. Training	Segment:
Phone #	Loc: Albuquerque	Time @ Hanford: na	Email:
Interviewer Dennis Walters	Date of Interview: 3/13/01		Reviewed
Industry Questions for Trade Contacts			
Question T1:	How is security awareness important to the success of your business?		
Reply:	Security is extremely important we support the Dept of Energy. Security is important to our customer. Our program covers the whole normal range of DOE security including transportation, computer, and information security. We do the initial security education and awareness training for new employees before they report to their first work-station. This is true except for a few cases where people work remotely from our general area. We also do the annual refresher training. There are about 300 people that we provide Security awareness training for.		
Question T2:	How do you manage the implementation of your security awareness program? - How do you train? - How do you evaluate the program? - How is your program developed?		
Reply:	<ul style="list-style-type: none"> - The new employee training is always given face-to-face. We like to put a face to security when new employees come on board. The first contact with security is during this initial training. We select security trainers who may have good people skills but are just friendly, easy to get along with people. These trainers give the new employees a tour of the compound. The other day a new employee made a point to wave to me. We are the first people they get to know at their new work location. We get to bond with them before anyone else. It is a good thing for them to bond with security. - Security puts notices in the "Newsbreak" (a general information paper that comes out ever couple of weeks). We put up posters, when we can get them. We prepare security awareness puzzles. These are often done on a voluntary basis but are occasional required. We don't actually have a security website. We send them to a note or an email or provide a URL that references to our puzzles or other special information in the Newsbreak. If they get on line they will sometimes get something like an Ice scraper as sewing kit or key chain. Just something small but they seem to like getting these rewards. We get a good response to our crossword puzzles. - We have done our refresher on line. They can read the material and take an online test. Our workers indicate they like being able to do the computer training. When they are happy, we are happy. - We sometimes bring in speakers with fun security presentations during the year, between the annual refresher. Mixing the training up with guess presenters adds interest. We usually don't require attendance at these sessions, although sometime we do require managers to attend. (This us usually for the earlier sessions so that they will be able to encourage others to attend the later scheduled sessions.) - We build security slowly. We follow a customer model. But we don't administer security. The workers administer security. All you have to do is see how many of us there are and how many of them there are and you know that it has to be up to them. We can't make them follow security. - When there are problems we look for reasons we haven't been successful (For instance, if we were to find some blueprints being thrown away. We would go talk to the work group supervisor to try to understand how we might improve our delivery of the message. We don't look to punish anyone. We just want to be sure they can do their jobs and meet security requirements easily. We ask them how we can help them. - When an employee gets the wrong answer on the refresher test, the security manager discusses the wrong answers in a non-punishing, helpful way to be sure the individual understands the issues and why the security requirement is important. - The training effectiveness is verified by testing. We also use a survey. - We found that people wanted to see the results about the survey. Now we tell them what actions are being taken. We think this will increase willingness to participate because they will see how their inputs are used to improve the program. - Our training is mostly developed in house. This allows us to focus on things meaningful to us. Like property protection and equipment security. Because our workers spend time on the road and visiting remote locations they have to be more aware of the fact that they can't be careless with their equipment, or information security. They are constantly exposed to security issues because of the traveling around they are doing. 		
QuestionT3:	What have you done to build employee ownership? - What has worked well? - What hasn't worked well?		
Reply:	Mostly answered above.		
Extra Question	How is your relationship with the workforce?		
Reply:	We are a small group. We have an excellent relationship. We do the give-a-ways, we do a customer service		

	model, one of the security people gives the tour of the compound and turns them over to the supervisor. This is a bonding process. They wave to us because they have bonded with us. Our team is people- people. We are participating in all of the morale activities, charitable stuff, employee teams to be part of the culture. Cancer drive - chili lunch- It's not us and them. We have picked the right people to present the initial training. Total quality ISO 9000, and Integrated Safety Management. We are delivering security in the same way. It's easier and better being accepted and liked.
Question T4:	Is there something I haven't asked that you think is important for me to know?
Reply:	
Question T5:	If I do only one thing to increase employee ownership of security, what should I it be?
Reply:	
Request for additional information	I would really appreciate getting electronic copies or web links to the following if you have them available.
	Some samples of promotional information you are using (maybe a few Newsbreaks, and anything you may be create for staff meeting information)
	(Am I right that you don't have a measure for security awareness?)
	A copy of the survey you use to get feedback and the summary results if possible.
	Samples of the Crossword.
	Anything else you might have that would help us to understand what you are doing to keep ownership with the workers.

A.9

Marketing Analysis and Strategy Formulation for Project Hanford Security Education and Awareness Program			
Interviewee:	Company:	Title:	Segment: TRADE Security Representative
Phone #	Loc: DOE - Pantex	Time @ Hanford:	Email:
Interviewer Dennis Walters	Date of Interview: 3/19/01	(Central Time Zone) 11:00 am	Comments coming
Industry Questions for Trade Contacts			
Question T1:	How is security awareness important to the success of your business?		
Reply:	What we do is assemble and disassemble nuclear warheads. Security and safety is vital. We must protect nuclear materials and the technology of the warheads. Our mission is the same as it was 40 years ago.		
Question T2:	How do you manage the implementation of your security awareness program? - How do you train? - How do you evaluate the program? - How is your program developed?		
Reply:	<ul style="list-style-type: none"> - Our security awareness program is base on briefings. We do not train. We hit the highlights of the topic. We tell them what kinds of information they need to be aware of, but the actual training takes place in their workplace. We expect them to take the requirements we discuss and learn to apply them using the subject matter experts and supervision available to them. We do the initial briefing on the first day. Once the employee is cleared, the employee receives another comprehensive briefing that relates to the specific job they will be doing. The requirements for the initial and comprehensive briefings are dictated in DOE Orders. We use face-to-face briefings on the initial and comprehensive. There are plant standards for security awareness program that identifies expectations and penalties such as loss of badge. - Each of us must attend all the training in the month of our birthday. Retraining is up to us. We can use infractions to help identify topics to cover in the retraining. For example: if safes are left open, or computer security is seen as a problem they will be added to the retraining. We are using CBT for the retraining - We are developing a job specific security briefing for the workers that will be conducted between the supervisor and the employee showing them the safe, the door. This specific safety not theoretical. It is very practical. The supervisor will use a checklist that we provide to conduct an orientation briefing for the employee once they are in the work area. - We also do special briefings. Quarterly we do safety meetings and have been allowed to provide a security element that is bugging them. Such as: there have been times that they have put classified info onto unclassified computers because they don't understand the aspects of the project that were classified. We had some problems with how we were locking safes. In those types of cases we come out and clarify and help them understand how to do it right. We don't want that problem to ever happen again. Special briefings are also done on an ad hoc basis whenever there is a problem that may need instant intervention. Just before holidays we remind people to take an extra moment. We put out a monthly security bulletin. - I have all aspects of security in my direction. This allows me to use my experience to identify areas of the facility that may need to hear about certain types of security problems. - We took the opportunity to create a sign at the main gate. It contains a slogan. But we put up a huge new signs (Sylvia Lovelett) - We use some give away items like coffee cups and lanyards. When we find someone in the plant who is doing a really good job like implementing the protecting the classified matter collection and control process by properly stamping and marking, by having neat and clean and orderly record files. - We occasional buy a lunch for someone doing something extra for us such as helping us during an audit. - We have security bulleting boards. We have a glassed case with Operations security material and our other security stuff. We use posters from HQ. We update the cases on about a 60-day cycle. - We measure security awareness effectiveness by reviewing infractions. When they are doing the right things, infractions are low. Basically we have seen very low numbers of infractions. 		
	<p>Do you think there some aspect that is keeping the infractions low? I think its because we rely on face-to-face and supervisor-employee communications. We don't rely on read and sign. When people are willing to take the time to come and talk about security, then it must be important. They can see our level of conviction from our voice and body language and the time we are willing to spend with them.</p> <p>If a person makes a mistake, a read and sign protects the company, but when I can look them in the face there is more accountability. Technology can take away the personal element. This may be hurting security awareness some of the programs.</p> <p>Do you conduct any surveys? We use self-assessments but don't do surveys.</p>		

QuestionT3:	<p>What have you done to build employee ownership?</p> <ul style="list-style-type: none"> - What has worked well? - What hasn't worked well?
Reply:	<p>What works: Walking the spaces. A security program is only as good as the conviction of the people delivering the program. We want our people out in the field at least 4 hours per day. It is important that the workers know us. We are working cooperatively to help people be successful. We state clearly what is required in the security bulletin. Compliance is not optional. However, we are there to help make it possible to meet the security requirements. We make the requirement unequivocal, but we explain why it exists and help them meet the requirements. We are all part of the team. What didn't work: I don't think read and sign works well. It doesn't get the message across. Interactions are needed to fully understand and commit to doing the right thing. This year we used a CBT and used the "so you want to be a millionaire" approach to providing the briefing. We let them use three helps. Unfortunately, the computer links didn't work right before the training went into the field and we didn't get all the failure modes. The people got lost in the logic and the results showed that they didn't pass the training. It was a good idea that didn't get implemented well. As soon as we realized what was happening we let everyone know. We revised it.</p>
Extra Question	How would you characterize the relationship between security and the workforce?
Reply:	There are elements of security that really upset the people (especially those that take time) but the workers know we must do it. Our relationship is good.
Question T4:	Is there something I haven't asked that you think is important for me to know?
Reply:	Come to the April conference. Visit the trading post? (There will be about 60 of us there. Lots of opportunity to learn.)
Question T5:	If there were one thing that could be done to increase employee ownership of security, what would it be?
Reply:	The success of any security program is the conviction of the people in the program. I can't know how convinced they are without talking directly to them. It gives me an opportunity to demonstrate my level of commitment and allows me to see their level of commitment for security.
Request for additional information	I will ask for some samples of promotional information you are using (for instance, the last few bulletins and staff meeting information)

A.10

Marketing Analysis and Strategy Formulation for Project Hanford Security Education and Awareness Program			
Interviewee:	Company: National Nuclear Security Administration (NNSA)	Title:	Segment: TRADE Security Representative
Phone #	Loc: Oakland Operations Office	Time @ Hanford:	Email:
Interviewer Dennis Walters	Date of Interview:	3/8/01	reviewed
Industry Questions for Trade Contacts			
Question T1:	How is security awareness important to the success of your business?		
Reply:	<p>We have about 400 people. This includes NNSA and our support contractors. Security is important to us because individuals need to know how to protect national security information and other sensitive information that may not be classified. Security also includes protecting facilities, equipment and people. We emphasize aspects of security based on the kinds of security incidents we are having. For example, if laptop computers or other equipment were to be taken from facilities where security badges are required, we will emphasize the need to control visitors and prevent "piggy backing" (allowing an individual to catch the door before it closes so that they can gain access without authorization). Another example that may be used is if an individual disposes of sensitive information in the trash such as social security numbers of employees we will prepare some sort of communication emphasizing the need to protect personal information. The NNSA Security Officer or Safeguards and Security Program usually notifies me. Sometimes they provide me with information, and other times I provide them with information for their approval about the topics to be covered and I prepare the information.</p>		
Question T2:	<p>How do you manage the implementation of your security awareness program?</p> <ul style="list-style-type: none"> - How do you train? - How do you evaluate the program? - How is your program developed? 		
Reply:	<p>We rely on a monthly bulletin to maintain general security awareness. If there is a need to put out a special bulletin we will. We also prepare information for managers to use in their staff meetings. Everyone must go through annual security training. We do all our annual training in April. This year we will be training for about 1.5-3 hours because the security program managers want to discuss their program issues directly with the workforce (DOE/support contractor). We also publish the NNSI security briefing that is available on the web to support any organization that wants security-training material. If the NNSI briefing does not meet our need, then we can provide a site specific briefing. People that miss the normal training can take the NNSI training to meet their annual requirement. New employees are given an employee handbook with security information.</p> <p>There is one FTE who provides Security Awareness and Foreign Travel support. This individual ensures that the posters that headquarters sends out to the field are posted. It's time consuming, but the posters are getting up as we receive them.</p> <p>We evaluate our training program by conducting customer feedback surveys. We find out what the participants liked or disliked about the training and what information they felt would help the next training.</p> <p>We develop the training through coordination with SSD Program Managers. The group includes the security program managers and the representative from Counterintelligence and Classification, and Export Control. (These are from outside our organization). The input we receive in our feedback is also used to help plan the training. One important source of training information comes from the Security Education Special Interest Group (SE-SIG). Networking is important to us because we have a limited budget and can use the help from others who are dealing with similar situations. Our training approach seems to be working well for us. We make a few changes to improve but the basic training is pretty good.</p>		
Question T3:	<p>What have you done to build employee ownership?</p> <ul style="list-style-type: none"> - What has worked well? - What hasn't worked well? 		
Reply:	<p>What works:</p> <p>The way we build ownership is to let them know it's their responsibility. We tell them it's their responsibility to protect their worksite. I try to be seen by the workforce at least annually (I wish it could be more often) so they will know that security is not just a program. I am working to help them. My most important message is that we must work together to make security work. It is difficult to keep security on their minds. We have a limited budget. We do what we can with what we have. They have to make security work. Also networking with other security awareness trainers is very important us. We need to help each other. This year my security awareness theme is "Coming Together to Make Security Work."</p> <p>This isn't something we did but you want to talk to Pantex One year they used a CD-rom for their security</p>		

	<p>awareness training. They completed a video of the program managers and other key people in security. This helped the workforce to know who the security support people were and what each program involved.</p> <p>What didn't work:</p> <p>Actually, there is only one thing that comes to mind. We had been doing computer-based briefings for about two years. Then we decided we needed to meet face-to-face for the training. The training was well received overall but there were some who would rather just do the computer-based briefings. They seem to like getting the computer-based briefings because of the convenience of completing at their desk. I would say don't get into a routine where people know what to expect.</p>
Request for additional information	I would really appreciate getting electronic copies or web links to the following if you have them available.
	Some samples of promotional information you are using (maybe the last few bulletins and staff meeting information)
	Can you let me know what indicators or performance measures you are using for determining security awareness (not the actual measurement value, just the information that is being measured and the performance criteria used. For example, what is acceptable and outstanding performance?)
	A reference to the Website for NNSI annual refresher training
	A copy of the survey you use to get feedback and the summary results if possible.
Question T4:	Is there something I haven't asked that you think is important for me to know?
Reply:	No.
Question T5:	If there were one thing that could be done to increase employee ownership of security, what would it be?
Reply:	You have to let people know that they are a part of it and must get involved. They are reliant on each other. We must all work together. We have a part in protecting each other. This is your program.
Feedback on how to improve the interview	The questions were fine.

A.11

Marketing Analysis and Strategy Formulation for Project Hanford Security Education and Awareness Program			
Interviewee:	Company:	Title: Security Trainer	Segment: TRADE Security Representative
Phone #	Loc: INEEL	Time @ Hanford:	Email:
Interviewer Dennis Walters	Date of Interview: 3/16/01		Sent - no comment received
Industry Questions for Trade Contacts			
Question T1:	How is security awareness important to the success of your business?		
Reply:	To impart knowledge and to help employees to keep a safe work environment. It's important to us because we're getting ready to have foreign nationals come here. This means we need to ensure people know about how to protect sensitive information. We also have to ensure that people have badges, don't bring prohibited items on site, know how to protect sensitive information, understand computer security. Know how to protect safeguards materials.		
Question T2:	How do you manage the implementation of your security awareness program? - How do you train? - How do you evaluate the program? - How is your program developed?		
Reply:	<p>Formal Training:</p> <ul style="list-style-type: none"> - We have required refresher training courses. We use computer based training for the refresher training. In some cases, where people work in remote sites that do not have a computer network connection we use a read and sign approach. We do some face-to-face training. Particularly for training for escorting of foreign nationals and for subcontractor escort training. New employee training is also delivered face-to-face. This is scheduled training that is presented weekly. New contractor, or visitors, can either view a video or attend the weekly face-to-face training. - Special training is done on an as requested basis. This includes targeted, short training of about 30 minutes duration. We generally use electronic slides in a Power-point presentation. We ask questions of the participants during the training to get them involved and to see that they understand the training. It is difficult to get the level of involvement we would like. It is easier to get more interaction during the training I do in Boy Scouts than with employees. It's really hard to engage the workers. We tend to have to rely on lecture for some of the specific information we need to communicate. The computer-based training does provide some opportunity for interaction. <p>Awareness Activities:</p> <ul style="list-style-type: none"> - We have an annual security contest to develop a new logo and slogan for security. We will give out a prize for the best logo and slogan. Some people will go to great lengths to do our whole function. - We will bring in outside speakers when we can afford to. We have lost some funding due to increased emphasis on counterintelligence training. But the counterintelligence group will bring someone in. - We are doing a summer project this year that is exciting. There will be a cubicle with all types of security discrepancies. People will be able to walk into the cubicle. One of the facilities did this and had great success. It gives people a chance to see, physically interact and discuss the security discrepancies they see in the cubicle. I have overheard people in the lunch room discussing what they saw. This exhibit has been wonderfully received. We have a committee of the contractors the ISEAT, INEEL, Security education and awareness team that usually meets quarterly unless there is a need to meet more often. They are developing a traveling exhibit. This is a fun way for people to learn. It's more hands. - Things to give away: We don't have many of the usual small gifts to give away because of budget cuts. But we do have a calendar that comes on in October, it is sent to the site, with our logo and slogan on it. The current one has a picture of an eagle with a man in a suit being held in its talons. The slogan reads, "You were saying this security stuff was for the birds?" - We always have a security article in the INEEL site paper. - We periodically send information through I-notes (an email/electronic newsletter) For instance last summer the heat was causing security badges to delaminate when they were being left in people's cars after work. We sent out a reminder about not leaving the badges in the cars. Sometimes there is a building where badges aren't being worn, or people might piggyback into the building. We will focus our information to the occupants of the building. There are seasonal reminders like when hunting season starts, we remind people about prohibited items such as guns and ammunition. Another situation is if there are computer viruses. The I-notes give us quick response capability for sending out a security message. - We have a one-page newspaper that is displayed in the restroom cubicles. We sometimes get to put things in this newspaper. These papers have a variety of information. They were started as part of our Safety program (VPP). The workers like the information that is in this newspaper. 		

	<p>How is security awareness similar or dissimilar to the safety program?</p> <p>Safety and Security go hand in hand. They are like two fingers on the same hand. But they should be kept separate because the types of things people need to do in safety and security are different. There are some similarities in how the information is communicated, but the approach is different. Safety (VPP) has more emphasis on requiring workers to conduct safety reviews like in safety walkthroughs.</p> <p>Performance awareness is measured,</p> <p>We give out security infraction when there are breaches in security. We needed to be able to show what we are doing to see that people understanding their responsibilities. The infractions are tracked. When they occur, we send out a hyperlink to a training module. When the training is completed we get a message. We have not done any surveys.</p> <p>Development: In the past we have done all the training development ourselves, but now training is getting more involved in the development of lesson plans and graphics.</p>
QuestionT3:	<p>What have you done to build employee ownership?</p> <ul style="list-style-type: none"> - What has worked well? - What hasn't worked well?
Reply:	<p>The traveling security cubical exhibit, computer based training (CBT), allowing individuals to do CBT refresher training at their convenience help build ownership and awareness. The logo/slogan development is really popular and gets hundreds of ideas some people have really worked hard developing graphics.) We do not allow any security people to give ideas.</p>
Extra Question	<p>How would you characterize the relationship between security and the workforce?</p>
	<p>We are probably considered by the site to be outsiders. Physical security, (guards, guns, gates) Personnel Security, (theft, waste, fraud), Technical security (National Security stuff). I think it has to be that way. We care a burden of secrecy because we see and have to act on the things that people do that are bad.</p>
Question T4:	<p>Is there something I haven't asked that you think is important for me to know?</p>
Reply:	<p>No, you have covered it. If I think of anything else I will share it with you.</p>
Question T5:	<p>If there were one thing that could be done to increase employee ownership of security, what would it be?</p>
Reply:	<p>To get people to make the correct choices. It's really sad when we do backgrounds and see how people have created problems for themselves. They need to stop violating the rules. I would try to get people to think before they make a choice. To get them to consider the impact of their actions.</p>
Request for additional information	<p>I would really appreciate getting electronic copies or web links to the following if you have them available.</p>
	<p>Some samples of promotional information you are using (the INEEL site paper, the I-notes, the one-page newspapers that are posted in the restrooms.</p>
	<p>Anything else you might have that would help us to understand what you are doing to keep ownership with the workers.</p>

A.12

Marketing Analysis and Strategy Formulation for Project Hanford Security Education and Awareness Program			
Interviewee:	Company:	Title:	Segment: TRADE Security Representative
Phone #	Loc: Pantex	Time @ Hanford:	Email:
Interviewer Dennis Walters	Date of Interview: 3/20/01		Reviewed
Industry Questions for Trade Contacts			
Question T1:	How is security awareness important to the success of your business?		
Reply:	<p>There are many aspects to security. There is control of sensitive information (the privacy act). Our main responsibility in Security Awareness is to ensure that people know they are in position of trust. We help them be aware of what they can and cannot talk about. The Awareness program ensures Operational Security (OPSEC) is maintained. Inside the fence we need to stay aware of the people we work with. We need to ensure that visitors don't get information that can be used against. To ensure this, there is information we cannot disclose.</p> <p>Security needs to be practiced in our homes as well. When we go on vacation, How we us our voice mail. We need to be aware that others can listen in on our cell phones. The can learn information about us that can be useful to them in harming us. In security awareness culture people understand and consider the potential consequences of security infractions both at work and at home.</p> <p>For instance, we get credit card applications that come in the mail. If we just toss them out in the trash, someone can retrieve them and use them to gain a credit card in our name that they can use.</p>		
Question T2:	<p>How do you manage the implementation of your security awareness program?</p> <ul style="list-style-type: none"> - How do you train? - How do you evaluate the program? - How is your program developed? 		
Reply:	<p>(Marvin Thompson interview provides most detail) One element of training I am please with is the retraining we did last year. We did a take off on "Who wants to be a millionaire?" called "Who wants to be security aware?" We have a broad range of people that we are communicating to. We have to appeal to the whole range with the information we present. I try to make it fun and interesting. I have used video to show some scenes with wrong things being done then the same scenes with right things being done. People really like CBT. We can log in from our office rather than go to a training lab. Its about a 10 minute session.</p> <p>I personalize and make security real by using examples of what has happened to me or what has happens to others.</p> <p>Part of our security message is that a clearance doesn't confer trust. People change or get into situations that can make them act unacceptably. We use behavioral interview techniques when hiring new people.</p> <p>We need to help people identify potential security problems. We have a hot line to allow them to make anonymous contact. People are often afraid to tell about concerns they may have. They people don't want to get involved or be hurt. They are afraid they won't be liked. People aren't usually aware of the way are acting.</p>		
QuestionT3:	<p>What have you done to build employee ownership?</p> <ul style="list-style-type: none"> - What has worked well? - What hasn't worked well? 		
Reply:	<p>What works: What didn't work: Lectures aren't good.</p>		
Extra Question	How would you characterize the relationship between security and the workforce?		
Reply:	Very good. People need us. The "track system" keeps us linked on training needs. We support the people by providing the briefings and retraining. I also do audits to see that they all have taken the courses they need.		
Question T4:	Is there something I haven't asked that you think is important for me to know?		
Reply:	No, not that I can think of. But if you need something else, just let me know.		
Question T5:	If there were one thing that could be done to increase employee ownership of security, what would it be?		
Reply:	I haven't been asked that before. Security starts from the very beginning. When their background is being checked, I tell them, "don't work about the clearance. But remember that honesty works best. It pays off in the long run."		

Request for additional information	I would really appreciate getting electronic copies or web links to the following if you have them available. Thanks Dennis.
	Some samples of promotional information you are using (maybe the last few bulletins and staff meeting information)
	Other materials that will help us understand how you are communicating security awareness and attempting to gain commitment for security requirements.

A.13

Marketing Analysis and Strategy Formulation for Project Hanford Security Education and Awareness Program			
Interviewee:	Company: Wackenhut	Title:	Segment: TRADE Security Representative
Phone #	Loc: ORNL	Time @ Hanford:	Email:
Interviewer Dennis Walters	Date of Interview:	3/26/01	Reviewed
Industry Questions for Trade Contacts			
Question T1:	How is security awareness important to the success of your business?		
Reply:	As part of our contract we provide support to the Department of Energy Oak Ridge Operations Office (DOE-ORO) complex for the Security Awareness program as required by DOE directives. Sensitive information needs to be protected. People need to understand the potential impact when they unintentionally release sensitive unclassified information.		
Question T2:	How do you manage the implementation of your security awareness program? - How do you train? - How do you evaluate the program? - How is your program developed?		
Reply:	<p>We have Certified instructors provide the security briefings. We strictly follow the DOE Order requirements for the topical areas. An Initial Security Briefing is required for each new employee who requires a badge. Each of the sites we support in this program has different site-specific information that is added to the basic Initial Security Briefing. The Annual Security Refresher briefing is accomplished by use of the WSI-OR website, on CDs, diskettes, in person, and in-group sessions. We tailor the delivery to meet the organization's needs. Mostly, the Initial & Comprehensive briefings are delivered through presentations by our Security Awareness staff.</p> <p>The Annual Security Refresher briefing is developed by the Oak Ridge Institute of Science and Education under a DOE Headquarters contract. They develop the basic briefing and provide it to the Nonproliferation and National Security Institute in Albuquerque, NM. NNSI finalizes the briefing and makes it available to the DOE complex. Then with the assistance of the DOE-ORO Security Awareness Program Manager, we tailor it to the specific needs of the complex. Last year's was over 225 pages of text. We trimmed it to 25 pages for delivery to the complex. Even then we received many complaints that it was too lengthy and took too much time to complete.</p> <p>We have people who have disabilities and we have to understand their needs when presenting a security briefing. We also present special security briefings as required. When providing a briefing, it has to be written so that all employees can understand it.</p> <p>In the new requirements (CY 2001), there is a requirement for a job specific briefing. We are concerned with how this will be done.</p> <p>Evaluation: We have discovered many new lessons from this first time in providing the Annual Security Refresher briefing. We have been gathering information for our database on problems encountered. We are putting together a customer satisfaction survey to gather comments on the quality of our training.</p> <p>We use posters for OPSEC and Security ED, Security Newsletters, and sites newsletters to augment security awareness. We have handouts we provide to other organizations within the DOE-ORO complex. We provide OPSEC briefings to various groups within each site. We provide briefings for escorts during International Atomic Energy Agency (IAEA) inspections of facilities at DOE-ORO sites. We can be contacted via email and hotline specifically for Security Awareness.</p>		
Question T3:	What have you done to build employee ownership? - What has worked well? - What hasn't worked well?		
Reply:	<p>What works:</p> <p>Our contract started effective January 10, 2000. When we got here people were required to get retrained each time they transferred from one facility to another one, while within the DOE-ORO complex. There was a variance in place regarding this training procedure. It was suggested that a clarification be obtained from DOE HQs on the wording of the Order. This was accomplished and DOE HQs agreed that a variance was not required. As a result of this clarification, it will save many hours of contractors sitting through the same security briefing.</p> <p>Another element of our program that is very effective is that we provide a variety of delivery approaches. CD, person-to-person, website and in groups.</p> <p>What didn't work:</p>		

	The results of the Annual Security Refresher Briefing, when completed on the website, is automatically entered into our database. We then download this database to a training point of contact at each site within the complex. Each site security manager has the responsibility of ensuring their personnel are completed the training in a timely manner. There have been numerous problems encountered with getting refresher training done on time.
Extra Question	How would you characterize the relationship between security and the workforce?
Reply:	Its good. The perception is that Scientists and Physicist sometimes consider security as a hindrance in their research. This is a problem we must correct. The perception is that they see security as a barrier when it comes to the exchange of scientific information with other scientists.
Question T4:	Is there something I haven't asked that you think is important for me to know?
Reply:	Not that I can think of. If I think of something I will talk with your team during the SE SIG in April.
Question T5:	If there were one thing that could be done to increase employee ownership of security, what would it be?
Reply:	Show them the threat we face at each site when it comes to the disclosure of sensitive unclassified information. This should include current examples. Some sources of information include, the Extranet for Security Professionals (ESP), the Security Policy Board, DOE resources. Stefan Leader, as part of the Office of Safeguards and Security under the direction of Toby Johnson, provides a monthly newsletter that contains unclassified threat information that is available to the sites.
Request for additional information	If possible, I would appreciate some samples of promotional information you are using (maybe the last few security newsletters, articles and staff meeting information)

A.14

Marketing Analysis and Strategy Formulation for Project Hanford Security Education and Awareness Program			
Interviewee:	Company:	Title:	Segment: Contr Mid. Lvl. Mgmt
Phone #	Loc:	Time @ Hanford: 4 ½ Years	Email:
Interviewer: Alison Marcum	Date of Interview: 3-26-01		
Interview Summary			
Highlights of Interview			
Question 1:	Have you ever held a security clearance?		
Reply:	No		
Question 2:	What changes in security awareness and ownership requirements have you seen?		
Reply:	- There was an escalation two years ago as a result of the Los Alamos incidents		
Question 3:	How important is security awareness and ownership at Hanford?		
Reply:	- It seems to be very important - Sometimes overboard		
Question 4:	Where, at Hanford, is security awareness and ownership most important? (Where should the program focus its energy?)		
Reply:	- PFP		
Question 5:	How important is security awareness and ownership in your area?		
Reply:	- Very (office security)		
Question 6:	What do you estimate your own awareness of security procedures and requirements to be? - What could be done to improve your awareness?		
Reply:	- Adequate-doesn't "profess to be an expert," but knows what is required for her work		
Question 7:	What elements of security awareness and ownership do you perceive to be of little value?		
Reply:	- Badges-too restrictive; where people have to wear them on their bodies, for example		
Question 8:	What security awareness and ownership issues do you find to be most important?		
Reply:	- She's not around information that would threaten national security; if she was, she'd certainly follow any necessary guidelines for protecting it - Believes that blanket procedures are not necessary for all areas		
Question 9:	What other management priorities compete with managing security awareness and ownership requirements?		
Reply:	- Security doesn't compete; she's responsible as part of her job for ensuring people are authorized and badged - Doesn't spend an excessive amount of time on it; most time is spent getting people badged, sometimes on short notice		
Question 10:	What are the criteria for having outstanding security awareness and ownership?		
Reply:	- Knowledge of restrictions, such as badging procedures		
Question 11:	How effective is the current program? - What elements of the program are most successful? - What elements could be improved upon?		
Reply:	- Believes it is effective - Most successful: none more successful than others - Could be improved: the program is too far reaching; example: she has a computer in her office that contains absolutely nothing that would be of any threat if it were retrieved by the wrong person, but since it's a DOE computer, no one can come into her office without proper badge and authorization		
Question 12:	Which programs do you perceive to be most successful in gaining active employee participation?		
Reply:	- Safety-a priority at every meeting		
Question 13:	What tools (i.e. types of information, communication methods) do you need in order to build commitment? - Do you feel you have those necessary tools? - If not, what do you feel you might need?		
Reply:	- She believes it is engrained in her staff, and they don't ever challenge it; so she doesn't need anything more		
Question 14:	If you were running the security awareness program at Hanford, what would you do to improve awareness and ownership?		
Reply:	- Use real-life examples - "This person got this information, and this is how it could or did hurt us" (Example)		

	- Re-examine whether or not certain rules and restriction need to be in place
Question 15:	How do you emphasize security awareness to your employees? - What are some of the hassles you face in communicating security program information to your employees?
Reply:	- It's not a daily topic - If she sees potential problems, she acts - Sees good pattern of compliance from her employees
Question 16:	What frustrations do you have, if any, regarding employee compliance with the security awareness and ownership program guidelines? - How does that affect you as a manager?
Reply:	- None
Question 17:	Do you think your employees have frustrations about security awareness and ownership? - If so, what are those frustrations related to?
Reply:	- They don't say they have any frustrations; they're very used to security
Question 18:	What are the consequences for failing to comply with security awareness and ownership program guidelines?
Reply:	- Depends on breach; disciplinary to termination
Question 19:	What are your employees' perceptions about the problems with security awareness and ownership?
Reply:	- There are no problems in her team - People are aware of security procedures and follow them
Question 20:	What kinds of security awareness and ownership-related media have you seen? - Have you seen posters or calendars? - Have you seen computerized messages, such as animated banners? - Have you seen the Security Ed cartoons?
Reply:	- Not a lot since Los Alamos incidents - She's so used to them, she doesn't notice them anymore - Aided: does not read Hanford Reach - See "Additional Notes" section at end of interview
Question 21:	Do you have a preference as to which kinds of media you enjoy seeing?
Reply:	- No; if something needs changing, she'd rather hear it verbally
Question 22:	Which of the security awareness and ownership materials are the most effective? Least effective? Why?
Reply:	- See "Additional Notes" section at end of interview
Question 23:	Is there something I haven't asked that you think is important for me to know?
Reply:	- No
Question 24:	If there were one thing that could be done to increase employee ownership of security, what would it be?
Reply:	- ???
Question 25:	Who else should I talk to?
Reply:	- Mike Berglund
Additional Notes:	- I did not go further into her awareness/preferences regarding security-related media (aided and unaided recall) as I perceived her as being slightly detached from security in general-she didn't elaborate on these kinds of questions and was clear that she didn't really notice any of these materials anymore to be able to recall what she's seen in a given period of time

A.15

Marketing Analysis and Strategy Formulation for Project Hanford Security Education and Awareness Program			
Interviewee:	Company: FH	Title:	Segment: Contr Mid. Lvl. Mgmt
Phone #	Loc: MO969 100K	Time @ Hanford: 18 Years	Email:
Interviewer: Alison Marcum	Date of Interview: 3-13-01		
Interview Summary			
Highlights of Interview			
Question 1:	Have you ever held a security clearance?		
Reply:	Yes		
Question 2:	What changes in security awareness and ownership requirements have you seen?		
Reply:	<ul style="list-style-type: none"> - Not sure he's seen any difference - No difference in importance 		
Question 3:	How important is security awareness and ownership at Hanford?		
Reply:	- Extremely		
Question 4:	Where, at Hanford, is security awareness and ownership most important? (Where should the program focus its energy?)		
Reply:	<ul style="list-style-type: none"> - New employees as they come on board - Should focus more on foreign nationals, especially with the diversity of the workforce currently employed 		
Question 5:	How important is security awareness and ownership in your area?		
Reply:	<ul style="list-style-type: none"> - Extremely - A day doesn't go by that his facility isn't reminded that security is important, especially with all of the patrol people around 		
Question 6:	What do you estimate your own awareness of security procedures and requirements to be?		
Reply:	<ul style="list-style-type: none"> - What could be done to improve your awareness? - You can always make improvements - Important to use examples; lessons learned from incidents at Hanford as well as other facilities are helpful 		
Question 7:	What elements of security awareness and ownership do you perceive to be of little value?		
Reply:	<ul style="list-style-type: none"> - None that he believes - Some issues are more nebulous than others, and therefore may not be as awareness-promoting; but everything is valuable 		
Question 8:	What security awareness and ownership issues do you find to be most important?		
Reply:	<ul style="list-style-type: none"> - Maintaining the security posture within his facility, which is harder recently due to construction people being there; important for non-Hanford site-related workers who aren't familiar with the whole security culture connected to work at the Hanford site to know the importance of following procedures 		
Question 9:	What other management priorities compete with managing security awareness and ownership requirements?		
Reply:	<ul style="list-style-type: none"> - Budget, schedule, everyday employee issues - Everyone is responsible for security, just as they are for safety; he places the responsibility on his employees 		
Question 10:	What are the criteria for having outstanding security awareness and ownership?		
Reply:	<ul style="list-style-type: none"> - People need to think security - Important for people to be aware of things that are going on around them at all times, and question those things that don't seem right - He thinks Hanford currently has a great security culture 		
Question 11:	How effective is the current program?		
Reply:	<ul style="list-style-type: none"> - What elements of the program are most successful? - What elements could be improved upon? - Most effective: good procedures; effective information program (including web site and training) - Could be improved: Within operations organization-when people come in from outside to support various activities, they should be targeted to make sure they understand security guidelines as well as insiders 		
Question 12:	Which programs do you perceive to be most successful in gaining active employee participation?		
Reply:	<ul style="list-style-type: none"> - Safety program-regardless of the work people do, they have to go home healthy and safe every day; the program is stressed so much that it carries over to their lives outside of work 		
Question 13:	What tools (i.e. types of information, communication methods) do you need in order to build commitment?		
Reply:	<ul style="list-style-type: none"> - Do you feel you have those necessary tools? 		

	- If not, what do you feel you might need?
Reply:	- He operates in a dynamic environment-one incident in one day can change everything, so it's hard to know exactly what is needed until something happens - Gave the example of the recent earthquake in the Seattle area-it happened all of a sudden, and caused he and his crew to spend four hours of intensive work to verify that everything in his facility was okay - Day to day, he feels he has the necessary tools to support security
Question 14:	If you were running the security awareness program at Hanford, what would you do to improve awareness and ownership?
Reply:	- See question 23
Question 15:	How do you emphasize security awareness to your employees? - What are some of the hassles you face in communicating security program information to your employees?
Reply:	- Security is discussed at regularly scheduled safety meetings; discussion includes information on changes and what they mean to the security posture; meetings used as a means of keeping everyone aware of what's going on in security; examples of "lessons learned" from incidents are also given when appropriate - Hassles: people sometimes feel that they're (security managers) are emphasizing something that isn't a risk; he sees the attitude of, "it takes so much to get into facilities; why worry once we're in?" - Complaints from employees wondering why they have to follow certain procedures, ones they don't feel are necessary to them
Question 16:	What frustrations do you have, if any, regarding employee compliance with the security awareness and ownership program guidelines? - How does that affect you as a manager?
Reply:	- None
Question 17:	Do you think your employees have frustrations about security awareness and ownership? - If so, what are those frustrations related to?
Reply:	- Security is one ancillary duty in a group of activities-employees aren't sure what they're supposed to focus on; there are too many other things to do besides worry about security guidelines - Also, see "Hassles" section of reply to question 15
Question 18:	What are the consequences for failing to comply with security awareness and ownership program guidelines?
Reply:	- It depends on the breach, but can range from verbal reprimand to termination
Question 19:	What are your employees' perceptions about the problems with security awareness and ownership?
Reply:	- ???
Question 20:	What kinds of security awareness and ownership-related media have you seen? - Have you seen posters or calendars? - Have you seen computerized messages, such as animated banners? - Have you seen the Security Ed cartoons?
Reply:	- Unaided: signs (along street) with security messages; has seen most via the web site (added that he was annoyed at first about having to start up his computer and see the Fluor Hanford Today messages, but has noticed this has been changed and is easier to bypass) - Aided: poster depicting badge types posted at his building entrance; hardly ever reads Hanford Reach; has never seen Security Ed
Question 21:	Do you have a preference as to which kinds of media you enjoy seeing?
Reply:	- No - After so much repetition of something, such as the banners on the web site, it becomes oblivious to people; he really doesn't look at it anymore
Question 22:	Which of the security awareness and ownership materials are the most effective? Least effective? Why?
Reply:	- No opinion on this - He does give high remarks to the Fluor Safeguards and Security web page, as he feels it is one of the better web pages on site and is easy to navigate
Question 23:	Is there something I haven't asked that you think is important for me to know?
Reply:	- No
Question 24:	If there were one thing that could be done to increase employee ownership of security, what would it be?
Reply:	- What he believes they are already doing-incentives - Believes incentives (money, award program, giveaways) motivate people and can improve behavior
Question 25:	Who else should I talk to?
Reply:	- Lou Simmons-River Corridor Project (he has a diverse background on and off site)

A.16

Interviewee:	Company: Duratek	Title:	Segment: Contr Mid. Lvl. Mgmt
---------------------	-------------------------	---------------	--------------------------------------

Phone #	Loc: 345HILLS RCHN	Time @ Hanford: 11 YEARS	Email:
Interviewer: Alison Marcum	Date of Interview: 3-15-01		
Interview Summary			
Highlights of Interview			
Question 1:	Have you ever held a security clearance?		
Reply:	- Has in the past, but does not hold one now		
Question 2:	What changes in security awareness and ownership requirements have you seen?		
Reply:	<ul style="list-style-type: none"> - Emphasis seems about the same as it always had - Has noticed a lessening of guards around the site 		
Question 3:	How important is security awareness and ownership at Hanford?		
Reply:	- Very		
Question 4:	Where, at Hanford, is security awareness and ownership most important? (Where should the program focus its energy?)		
Reply:	<ul style="list-style-type: none"> - Prevention of theft of government property: has noticed that this is an increasing problem. He sees people "around town" wearing clothing that says "Property of U.S. Gov't" and considers it theft since this attire is to be used while at work on the site, and is not to be taken home or worn outside of work. To him, this is theft. 		
Question 5:	How important is security awareness and ownership in your area?		
Reply:	<ul style="list-style-type: none"> - Not extremely, as he deals with very few things considered "Gov't confidential" and more things that are considered "company confidential. The areas he supports are for the most part unsecured. - He added that there are two rooms at the office he works at devoted to security – for meetings, etc. 		
Question 6:	<ul style="list-style-type: none"> What do you estimate your own awareness of security procedures and requirements to be? What could be done to improve your awareness? 		
Reply:	- He indicated that "for his job" not much could be done to improve his awareness		
Question 7:	What elements of security awareness and ownership do you perceive to be of little value?		
Reply:	- "None" – he thinks the current program is "about right."		
Question 8:	What security awareness and ownership issues do you find to be most important?		
Reply:	- Ensuring that people in facilities have a reason to be there		
Question 9:	What other management priorities compete with managing security awareness and ownership requirements?		
Reply:	<ul style="list-style-type: none"> - At first, he indicated that not much competes - Then he added the following: 1) Production issues (company proprietary rather than DOE); 2) Marketing – being able to explain enough about what they're doing without saying too much (a fine line) 		
	What are the criteria for having outstanding security awareness and ownership?		
Reply:	<ul style="list-style-type: none"> - Compared to non-Hanford general industry, he believes the culture is already much stronger - Need to continually re-enforce security through the use of signs, patrol, Hanford General Employee Training (HGET), etc. 		
Question 11:	<ul style="list-style-type: none"> How effective is the current program? What elements of the program are most successful? What elements could be improved upon? 		
Reply:	<ul style="list-style-type: none"> - Most successful: protection of secure materials, protection of nuclear materials - Least successful: protection of government property (see reply to Question 4 for further explanation) 		
Question 12:	Which programs do you perceive to be most successful in gaining active employee participation?		
Reply:	- There is a heavier emphasis on safety/health than on security – more people use safety/health standards in everyday life than security standards		
Question 13:	<ul style="list-style-type: none"> What tools (i.e. types of information, communication methods) do you need in order to build commitment? Do you feel you have those necessary tools? If not, what do you feel you might need? 		
Reply:	- Has what he needs – security is not as big of an issue in his particular area (as a subcontractor at a lower security office)		
Question 14:	If you were running the security awareness program at Hanford, what would you do to improve awareness and ownership?		
Reply:	- ???		
Question 15:	<ul style="list-style-type: none"> How do you emphasize security awareness to your employees? What are some of the hassles you face in communicating security program information to your employees? 		
Reply:	<ul style="list-style-type: none"> - Staff meetings – security is on the meeting agenda approximately once per month, and consists of little reminders about badges and locking of doors, etc. – can't really have them more often as his employees are 		

	<p>spread out all over, geographically and only come together for staff meetings twice per month</p> <ul style="list-style-type: none"> - Badges are checked heavily – a receptionist’s desk sits directly in front of entrance, and she checks every single person as they come and go <p>(*This person greeted me within 10 seconds after I entered the building, and issued a visitor’s badge after verifying my appointment with Mr. Smith. There were also signs posted at each hallway entrance that said, “Badges MUST be worn beyond this point.”)</p>
Question 16:	<p>What frustrations do you have, if any, regarding employee compliance with the security awareness and ownership program guidelines?</p> <ul style="list-style-type: none"> - How does that affect you as a manager?
Reply:	<ul style="list-style-type: none"> - Has none
Question 17:	<p>Do you think your employees have frustrations about security awareness and ownership?</p> <ul style="list-style-type: none"> - If so, what are those frustrations related to?
Reply:	<ul style="list-style-type: none"> - None expressed to him - He added that, “We tow the line tighter than staff inside the fence”
Question 18:	<p>What are the consequences for failing to comply with security awareness and ownership program guidelines?</p>
Reply:	<ul style="list-style-type: none"> - Being a subcontractor to DOE . . .if client says they are no longer welcome (possibly for excessive security incidents, for example), then they’re done
Question 19:	<p>What are your employees’ perceptions about the problems with security awareness and ownership?</p>
Reply:	<ul style="list-style-type: none"> - ???
Question 20:	<p>What kinds of security awareness and ownership-related media have you seen?</p> <ul style="list-style-type: none"> - Have you seen posters or calendars? - Have you seen computerized messages, such as animated banners? - Have you seen the Security Ed cartoons?
Reply:	<ul style="list-style-type: none"> - Unaided: posters, patrolmen - Aided: Has seen “Security Ed” cartoons but doesn’t pay attention; only visits the intranet once in 9 months, so has seen banners, but doesn’t really deal with them. His office isn’t connected to it, so he only sees its contents when visiting other offices
Question 21:	<p>Do you have a preference as to which kinds of media you enjoy seeing?</p>
Reply:	<ul style="list-style-type: none"> - “No, not really.” - Whatever it is needs to be really visible
Question 22:	<p>Which of the security awareness and ownership materials are the most effective? Least effective? Why?</p>
Reply:	<ul style="list-style-type: none"> - Most effective: posters, since there are more of them out there - Least effective: banners on intranet – not effective for him and his employees since they don’t have regular access to them
Question 23:	<p>Is there something I haven’t asked that you think is important for me to know?</p>
Reply:	<ul style="list-style-type: none"> - He took this opportunity to reiterate his “biggest beef” – people wearing government property – “If they take that, what else will they take?”
Question 24:	<p>If there were one thing that could be done to increase employee ownership of security, what would it be?</p>
Reply:	<ul style="list-style-type: none"> - “I can’t think of anything.” - Added that given the level of most jobs at Hanford, the security program meets what needs to be done - He’s been to other government as well as non-government sites that “aren’t as good as far as security is concerned.”
Question 25:	<p>Who else should I talk to?</p>
Reply:	<p>1) Dale Gregley, Bechtel Physics Manager; and 2) Mike Hood, Bechtel Field Support Manager (all craft people)</p>
Additional Notes:	<ul style="list-style-type: none"> - I noticed that in the lobby of the Duratek building, there was a board entitled “Safety Employee of the Month.” It included pictures and names of people who earned this award during the past six months and a plaque engraved with their names. It was interesting, however, that it had not been updated since October of 2000. - I did not notice any security-related media posted anywhere other than the signs at each hallway requiring badges to be worn.

A.17

Marketing Analysis and Strategy Formulation for Project Hanford Security Education and Awareness Program			
Interviewee:	Company:	Title:	Segment: Contr Mid. Lvl. Mgmt
Phone #	Loc:	Time @ Hanford: 20yr	Email:
Interviewer: Kevin Higginson	Date of Interview:		
Interview Summary			
Highlights of Interview			
Question 1:	Have you ever held a security clearance?		
Reply:	Yes		
Question 2:	What changes in security awareness and ownership requirements have you seen?		
Reply:	Security awareness has heightened since the end of the Cold War.		
Question 3:	How important is security awareness and ownership at Hanford?		
Reply:	It is very important to be observant; the biggest threat is the insider.		
Question 4:	Where, at Hanford, is security awareness and ownership most important? (Where should the program focus its energy?)		
Reply:	The biggest threat at Hanford (excluding PNNL) is sabotage. Hanford is in a clean-up mode, not a weapons production site. We still have tons of plutonium and uranium that are being stabilized and repackaged into safe containers. These items would pose an environmental threat if they were in the wrong hands. Therefore security awareness is very important.		
Question 5:	How important is security awareness and ownership in your area?		
Reply:	Very important.		
Question 6:	What do you estimate your own awareness of security procedures and requirements to be? - What could be done to improve your awareness?		
Reply:	Very good More internal audits by the Hanford security but do these audits to help the employees and not to just find security infractions		
Question 7:	What elements of security awareness and ownership do you perceive to be of little value?		
Reply:	I believe it is all-important.		
Question 8:	What security awareness and ownership issues do you find to be most important?		
Reply:	Security badging		
Question 9:	What other management priorities compete with managing security awareness and ownership requirements?		
Reply:	Time constraints in meeting deadlines It is at the top right next to safety It is at the top right next to safety Positive is following security procedure correctly and getting your job done, the negative is causing a security violation that generates paper and stops work		
Question 10:	What are the criteria for having outstanding security awareness and ownership?		
Reply:	Knowing the security procedures and rules in your work area, familiar with the work your doing, making sure that you have the proper badging for going into work areas and ask someone knowledgeable if you are unsure of any security issues.		
Question 11:	How effective is the current program? - What elements of the program are most successful? - What elements could be improved upon?		
Reply:	All All None		
Question 12:	Which programs do you perceive to be most successful in gaining active employee participation?		
Reply:	. All		
Question 13:	What tools (i.e. types of information, communication methods) do you need in order to build commitment? - Do you feel you have those necessary tools? - If not, what do you feel you might need?		

Reply:	More computer based training Yes
Question 14:	If you were running the security awareness program at Hanford, what would you do to improve awareness and ownership?
Reply:	
Question 15:	How do you emphasize security awareness to your employees? - What are some of the hassles you face in communicating security program information to your employees?
Reply:	Awards to employees for not having security infractions.
Question 16:	What frustrations do you have, if any, regarding employee compliance with the security awareness and ownership program guidelines? - How does that affect you as a manager?
Reply:	Weekly meetings None
Question 17:	Do you think your employees have frustrations about security awareness and ownership? - If so, what are those frustrations related to?
Reply:	None
Question 18:	What are the consequences for failing to comply with security awareness and ownership program guidelines?
Reply:	To many security requirements to do there jobs. To many security requirements
Question 19:	What are your employees' perceptions about the problems with security awareness and ownership?
Reply:	Time off without pay
Question 20:	What kinds of security awareness and ownership-related media have you seen? - Have you seen posters or calendars? - Have you seen computerized messages, such as animated banners? - Have you seen the Security Ed cartoons?
Reply:	- I do notice posters going into main building entrances. Yes, there are security messages sent to all employees on there computers
Question 21:	Do you have a preference as to which kinds of media you enjoy seeing?
Reply:	Video or computer
Question 22:	Which of the security awareness and ownership materials are the most effective? Least effective? Why?
Reply:	Computer generated security training is most effective I can take my time and relax why I 'm learning Training Classes-least
Question 23:	Is there something I haven't asked that you think is important for me to know?
Reply:	no
Question 24:	If there were one thing that could be done to increase employee ownership of security, what would it be?
Reply:	Awards for contributions to enhance the security program
Question 25:	Who else should I talk to?
Reply:	Security Awareness Program Manager

A.18

Marketing Analysis and Strategy Formulation for Project Hanford Security Education and Awareness Program			
Interviewee:	Company:	Title:	Segment: Contr Mid. Lvl. Mgmt
Phone #	Loc:	Time @ Hanford: 15yr	Email:
Interviewer: Kevin Higginson	Date of Interview:		
Interview Summary			
Highlights of Interview			
Question 1:	Have you ever held a security clearance?		
Reply:	Yes Q late 80's		
Question 2:	What changes in security awareness and ownership requirements have you seen?		
Reply:	My job requires me to be aware of employee security issues and computer security. The employee security general issues have become more informal and the employees are accountable or trusted more. The computer security has increased due to new technology and having world access. The most visible change is guards touching every badge for entry into a facility.		
Question 3:	How important is security awareness and ownership at Hanford?		
Reply:	The HGET training has improved greatly and is a great awareness tool. If employees are more accountable it is critical they know the security requirements. In the general work areas it is more property protection, use of government resources, fitness for duty, and computer security. Awareness is important and the employee's jobs depend on following the guidance.		
Question 4:	Where, at Hanford, is security awareness and ownership most important? (Where should the program focus its energy?)		
Reply:	Nuclear materials and safety risk areas. Anything that would prevent emergency personnel to respond to an event.		
Question 5:	How important is security awareness and ownership in your area?		
Reply:	My organization is responsible to protecting information and data integrity. This includes physical security to technology security. I believe my group is very aware. Several have Q clearance to operate the DOE Clearance Security. The system and Oracle administrator have all privileges and they know that is has high responsibilities.		
Question 6:	What do you estimate your own awareness of security procedures and requirements to be? - What could be done to improve your awareness?		
Reply:	General manager employee awareness plus high computer awareness Reporting requirements		
Question 7:	What elements of security awareness and ownership do you perceive to be of little value?		
Reply:	Richland buildings		
Question 8:	What security awareness and ownership issues do you find to be most important?		
Reply:	Keeping sensitive information confidential		
Question 9:	What other management priorities compete with managing security awareness and ownership requirements?		
Reply:	Responding and correcting system problems near the top First priority is to keep systems running no questions Administrative activities are a low priority I try to be there for my employees for work and personal issues		
Question 10:	What are the criteria for having outstanding security awareness and ownership?		
Reply:	There are no incidents or accidents that could have been prevented		
Question 11:	How effective is the current program? - What elements of the program are most successful? - What elements could be improved upon?		
Reply:	Good - every employee gets yearly training with HGET. HGET is simple and holds the interest of employees. Training is a graded approach and related to the job performed. Fitness for duty Some confusion as a non-prime contractor. Follow the same rules sometimes needs to have more information. As a long time employee, I have a different perspective from new employees. New employees are coming from a school environment to their first government business experience. It is critical to focus on new employees		
Question 12:	Which programs do you perceive to be most successful in gaining active employee participation?		
Reply:	. Computer based training		
Question 13:	What tools (i.e. types of information, communication methods) do you need in order to build		

	commitment? - Do you feel you have those necessary tools? - If not, what do you feel you might need?
Reply:	Professional employees who know the guidelines. Yes
Question 14:	If you were running the security awareness program at Hanford, what would you do to improve awareness and ownership?
Reply:	If employees have an appreciation of some of the reasons for guidelines it might get more buy-in. I realize we have to but if I know it is to protect family, home, and me I would be more zealous
Question 15:	How do you emphasize security awareness to your employees? - What are some of the hassles you face in communicating security program information to your employees?
Reply:	Security compliance is written in the job responsibilities The need for a standard approach so all employees perform the same tasks to the standard
Question 16:	What frustrations do you have, if any, regarding employee compliance with the security awareness and ownership program guidelines? - How does that affect you as a manager?
Reply:	None
Question 17:	Do you think your employees have frustrations about security awareness and ownership? - If so, what are those frustrations related to?
Reply:	No
Question 18:	What are the consequences for failing to comply with security awareness and ownership program guidelines?
Reply:	Depending on the failure we could be fired. Not knowing the guidelines is not excuse.
Question 19:	What are your employees' perceptions about the problems with security awareness and ownership?
Reply:	They know it is a no choice item. They will do what is required
Question 20:	What kinds of security awareness and ownership-related media have you seen? - Have you seen posters or calendars? - Have you seen computerized messages, such as animated banners? - Have you seen the Security Ed cartoons?
Reply:	No WEB Page from PTH is very good. The banner subjects are good refresh topics. They keep it in front of employees all the time
Question 21:	Do you have a preference as to which kinds of media you enjoy seeing?
Reply:	Computer based
Question 22:	Which of the security awareness and ownership materials are the most effective? Least effective? Why?
Reply:	People just don't response retain memos or handbooks.
Question 23:	Is there something I haven't asked that you think is important for me to know?
Reply:	no
Question 24:	If there were one thing that could be done to increase employee ownership of security, what would it be?
Reply:	
Question 25:	Who else should I talk to?
Reply:	

A.19

Marketing Analysis and Strategy Formulation for Project Hanford Security Education and Awareness Program			
Interviewee:	Company:	Title:	Segment: Contr Mid. Lvl. Mgmt
Phone #	Loc:	Time @ Hanford: 18yr	Email:
Interviewer: Kevin Higginson	Date of Interview:		
Interview Summary			
Highlights of Interview			
Question 1:	Have you ever held a security clearance?		
Reply:	Yes		
Question 2:	What changes in security awareness and ownership requirements have you seen?		
Reply:	More awareness in recent years.		
Question 3:	How important is security awareness and ownership at Hanford?		
Reply:	It is constantly being stressed and is very important.		
Question 4:	Where, at Hanford, is security awareness and ownership most important? (Where should the program focus its energy?)		
Reply:	At PFP where Plutonium is stored and wherever classified information exists.		
Question 5:	How important is security awareness and ownership in your area?		
Reply:	It is always a top consideration.		
Question 6:	What do you estimate your own awareness of security procedures and requirements to be? - What could be done to improve your awareness?		
Reply:	Very good Nothing		
Question 7:	What elements of security awareness and ownership do you perceive to be of little value?		
Reply:	None		
Question 8:	What security awareness and ownership issues do you find to be most important?		
Reply:	Safeguarding nuclear materials, wearing of badges that show clearances, auditing of safes.		
Question 9:	What other management priorities compete with managing security awareness and ownership requirements?		
Reply:	- Only from standpoint of general awareness and general observations - Safety has to come first, followed by security. Actually they go hand in hand.		
Question 10:	What are the criteria for having outstanding security awareness and ownership?		
Reply:	Everyone aware and practicing ownership		
Question 11:	How effective is the current program? - What elements of the program are most successful? - What elements could be improved upon?		
Reply:	Very effective - More information on security violations.		
Question 12:	Which programs do you perceive to be most successful in gaining active employee participation?		
Reply:	.The safety program with weekly meetings		
Question 13:	What tools (i.e. types of information, communication methods) do you need in order to build commitment? - Do you feel you have those necessary tools? - If not, what do you feel you might need?		
Reply:	Management commitment to put security before work Yes		
Question 14:	If you were running the security awareness program at Hanford, what would you do to improve awareness and ownership?		
Reply:			
Question 15:	How do you emphasize security awareness to your employees? - What are some of the hassles you face in communicating security program information to your employees?		
Reply:	Exchange information with employees None		
Question 16:	What frustrations do you have, if any, regarding employee compliance with the security awareness and ownership		

	program guidelines? - How does that affect you as a manager?
Reply:	None
Question 17:	Do you think your employees have frustrations about security awareness and ownership? - If so, what are those frustrations related to?
Reply:	Yes It should be targeted toward your own areas of responsibility; we don't need overkill
Question 18:	What are the consequences for failing to comply with security awareness and ownership program guidelines?
Reply:	Consequences are usually harsh with not much room for human error
Question 19:	What are your employees' perceptions about the problems with security awareness and ownership?
Reply:	
Question 20:	What kinds of security awareness and ownership-related media have you seen? - Have you seen posters or calendars? - Have you seen computerized messages, such as animated banners? - Have you seen the Security Ed cartoons?
Reply:	Posters, training classes, videos Yes
Question 21:	Do you have a preference as to which kinds of media you enjoy seeing?
Reply:	Videos of case studies that have occurred
Question 22:	Which of the security awareness and ownership materials are the most effective? Least effective? Why?
Reply:	Video tapes better than presentations or training classes
Question 23:	Is there something I haven't asked that you think is important for me to know?
Reply:	No
Question 24:	If there were one thing that could be done to increase employee ownership of security, what would it be?
Reply:	Weekly or monthly video tape
Question 25:	Who else should I talk to?
Reply:	

A.20

Marketing Analysis and Strategy Formulation for Project Hanford Security Education and Awareness Program			
Interviewee:	Company:	Title:	Segment: Contr Mid. Lvl. Mgmt
Phone #	Loc:	Time @ Hanford:	Email:
Interviewer: Kevin Higginson	Date of Interview:		
Interview Summary			
Highlights of Interview			
Question 1:	Have you ever held a security clearance?		
Reply:	Yes		
Question 2:	What changes in security awareness and ownership requirements have you seen?		
Reply:	Up and down depending on year.		
Question 3:	How important is security awareness and ownership at Hanford?		
Reply:	Very important. More emphasis over past two years.		
Question 4:	Where, at Hanford, is security awareness and ownership most important? (Where should the program focus its energy?)		
Reply:	In classified holdings and classified computer security.		
Question 5:	How important is security awareness and ownership in your area?		
Reply:	Very important, since I have both classified files and electronic media.		
Question 6:	What do you estimate your own awareness of security procedures and requirements to be? - What could be done to improve your awareness?		
Reply:	Very high Monthly updates in cc-mail, short and to the point.		
Question 7:	What elements of security awareness and ownership do you perceive to be of little value?		
Reply:	Information relating to areas of activity, that I am not involved with		
Question 8:	What security awareness and ownership issues do you find to be most important?		
Reply:	Safeguarding classified information.		
Question 9:	What other management priorities compete with managing security awareness and ownership requirements?		
Reply:	None Number one priority Security violations can result in loss of security clearance and possible loss of employment		
Question 10:	What are the criteria for having outstanding security awareness and ownership?		
Reply:	Clear and concise rules.		
Question 11:	How effective is the current program? - What elements of the program are most successful? - What elements could be improved upon?		
Reply:	Very good - Audits, daily guard checks. Vague rules and policies that are subject to interpretation		
Question 12:	Which programs do you perceive to be most successful in gaining active employee participation?		
Reply:	Safety Program		
Question 13:	What tools (i.e. types of information, communication methods) do you need in order to build commitment? - Do you feel you have those necessary tools? - If not, what do you feel you might need?		
Reply:	Knowledge of requirements, and equipment (repositories, and classified computers) that meet needs for storage and electronic processing. Yes		
Question 14:	If you were running the security awareness program at Hanford, what would you do to improve awareness and ownership?		
Reply:	- Provide weekly security information to be included as an add-on subject to the weekly Monday morning safety meetings.		
Question 15:	How do you emphasize security awareness to your employees? - What are some of the hassles you face in communicating security program information to your employees?		
Reply:	Lack of concern for a dry subject.		

Question 16:	What frustrations do you have, if any, regarding employee compliance with the security awareness and ownership program guidelines? - How does that affect you as a manager?
Reply:	Cutting corners to save time Potential loss of job
Question 17:	Do you think your employees have frustrations about security awareness and ownership? - If so, what are those frustrations related to?
Reply:	Yes Classification of material that previously was not classified several years earlier.
Question 18:	What are the consequences for failing to comply with security awareness and ownership program guidelines?
Reply:	Loss of clearances and jobs for both; poor performance ratings.
Question 19:	What are your employees' perceptions about the problems with security awareness and ownership?
Reply:	None, employees are very aware and take responsibility for their actions.
Question 20:	What kinds of security awareness and ownership-related media have you seen? - Have you seen posters or calendars? - Have you seen computerized messages, such as animated banners? - Have you seen the Security Ed cartoons?
Reply:	Cc-mail discussing violations and security problems throughout the U.S. Yes No
Question 21:	Do you have a preference as to which kinds of media you enjoy seeing?
Reply:	CC-mail is fine.
Question 22:	Which of the security awareness and ownership materials are the most effective? Least effective? Why?
Reply:	Frequent communication most effective; posters least effective.
Question 23:	Is there something I haven't asked that you think is important for me to know?
Reply:	
Question 24:	If there were one thing that could be done to increase employee ownership of security, what would it be?
Reply:	Add security as a topic for the weekly Monday morning safety meetings.
Question 25:	Who else should I talk to?
Reply:	Hanford Patrol, Hanford Safeguards and Accountability.

A.21

Marketing Analysis and Strategy Formulation for Project Hanford Security Education and Awareness Program			
Interviewee:	Company:	Title:	Segment: Contr Mid. Lvl. Mgmt
Phone #	Loc:	Time @ Hanford: 1yr 2mon	Email:
Interviewer: Kevin Higginson	Date of Interview:		
Interview Summary			
Highlights of Interview			
Question 1:	Have you ever held a security clearance?		
Reply:	Yes		
Question 2:	What changes in security awareness and ownership requirements have you seen?		
Reply:			
Question 3:	How important is security awareness and ownership at Hanford?		
Reply:	It is very important		
Question 4:	Where, at Hanford, is security awareness and ownership most important? (Where should the program focus its energy?)		
Reply:	It is important across the site		
Question 5:	How important is security awareness and ownership in your area?		
Reply:	Very important as I work in a higher security concern area		
Question 6:	What do you estimate your own awareness of security procedures and requirements to be? - What could be done to improve your awareness?		
Reply:	I am aware of what is expected of me Continue with current program		
Question 7:	What elements of security awareness and ownership do you perceive to be of little value?		
Reply:	I believe the site is too conservative in some aspects of the program		
Question 8:	What security awareness and ownership issues do you find to be most important?		
Reply:	Maintaining security is important		
Question 9:	What other management priorities compete with managing security awareness and ownership requirements?		
Reply:	They do not compete. Security, as with safety, is a constraint in the performance of my job - It is a part of all activities I perform in some way or another there are risks associated with every decision we make. Security issues are simply factors that go into the decision making process. I am not allowed to deviate from the security requirements so I manage within them		
Question 10:	What are the criteria for having outstanding security awareness and ownership?		
Reply:	Everyone understands the requirements and is accountable for those requirements		
Question 11:	How effective is the current program? - What elements of the program are most successful? - What elements could be improved upon?		
Reply:	Fairly effective		
Question 12:	Which programs do you perceive to be most successful in gaining active employee participation?		
Reply:	all employees attend the necessary training and comply with the requirements. I suppose compliance is active participation		
Question 13:	What tools (i.e. types of information, communication methods) do you need in order to build commitment? - Do you feel you have those necessary tools? - If not, what do you feel you might need?		
Reply:	I believe the methods used are effective at PFP, not sure about the rest of the site		
Question 14:	If you were running the security awareness program at Hanford, what would you do to improve awareness and ownership?		
Reply:	I would remove some of the computer links on the site web page that take people to web sites that are not work related. This seems to be a set-up for failure to the employee by making it appear they can visit those sites.		
Question 15:	How do you emphasize security awareness to your employees? - What are some of the hassles you face in communicating security program information to your employees?		

Reply:	Through briefings and actions (i.e. supporting the program when asked questions or the situation arises) None
Question 16:	What frustrations do you have, if any, regarding employee compliance with the security awareness and ownership program guidelines? - How does that affect you as a manager?
Reply:	It is frustrating when an employee makes a mistake. However, in my experience at PFP, every mistake was quickly followed by a self-reporting. This is a good thing. Takes time away from other tasks to spend with the employee and everyone else on the security issue
Question 17:	Do you think your employees have frustrations about security awareness and ownership? - If so, what are those frustrations related to?
Reply:	Yes, they believe they are too conservative
Question 18:	What are the consequences for failing to comply with security awareness and ownership program guidelines?
Reply:	Consequences are the same for failure to comply with all program requirements. Depends on the nature of the non-compliance and the contributing causes.
Question 19:	What are your employees' perceptions about the problems with security awareness and ownership?
Reply:	In some cases they do not take them as seriously as they should because they believe the program is too conservative and hard to comply with in many areas where the rule should be revised to minimize conservatism and make it easier for them to do their job. If you have too many requirements, and the interpretation of those requirements changes frequently (such as with the PSAP rules) it is a set-up for non-compliance
Question 20:	What kinds of security awareness and ownership-related media have you seen? - Have you seen posters or calendars? - Have you seen computerized messages, such as animated banners? - Have you seen the Security Ed cartoons?
Reply:	Posters, signs, newspaper articles, etc. Yes
Question 21:	Do you have a preference as to which kinds of media you enjoy seeing?
Reply:	No
Question 22:	Which of the security awareness and ownership materials are the most effective? Least effective? Why?
Reply:	Computer messages are interesting with the animated graphics (people with guns all over the place helps too). E-mail messages—I get too many every day for them to be very effective.
Question 23:	Is there something I haven't asked that you think is important for me to know?
Reply:	I work in the protected area of PFP, so my perception of security awareness is skewed to physical security requirements as we are inside the protected area.
Question 24:	If there were one thing that could be done to increase employee ownership of security, what would it be?
Reply:	Come out and talk with them about ways the security program could work with them to make their job easier
Question 25:	Who else should I talk to?
Reply:	Employees (operators, RCTs, SOEs, etc.)

A.22

Marketing Analysis and Strategy Formulation for Project Hanford Security Education and Awareness Program			
Interviewee:	Company:	Title:	Segment: Contr Mid. Lvl. Mgmt
Phone #	Loc:	Time @ Hanford:	Email:
Interviewer: Kevin Higginson	Date of Interview:		
Interview Summary			
Highlights of Interview			
Question 1:	Have you ever held a security clearance?		
Reply:	Yes		
Question 2:	What changes in security awareness and ownership requirements have you seen?		
Reply:	Fairly high awareness until the mid 90's when Hanford inventory quantities were being declassified. From 98 and thereafter saw a new emphasis placed on high security. With the spy scandals, awareness and enforcement of new security policies are a very high priority.		
Question 3:	How important is security awareness and ownership at Hanford?		
Reply:	Very high priority.		
Question 4:	Where, at Hanford, is security awareness and ownership most important? (Where should the program focus its energy?)		
Reply:	Wherever nuclear material or classified information is stored.		
Question 5:	How important is security awareness and ownership in your area?		
Reply:	The highest importance.		
Question 6:	What do you estimate your own awareness of security procedures and requirements to be? - What could be done to improve your awareness?		
Reply:	High Constant reminders		
Question 7:	What elements of security awareness and ownership do you perceive to be of little value?		
Reply:	None		
Question 8:	What security awareness and ownership issues do you find to be most important?		
Reply:	Compliance with storage and communication of classified material		
Question 9:	What other management priorities compete with managing security awareness and ownership requirements?		
Reply:	None - Compliance with security requirements is the foremost consideration Doesn't matter, security comes first		
Question 10:	What are the criteria for having outstanding security awareness and ownership?		
Reply:	Information, commitment, accountability, follow-up		
Question 11:	How effective is the current program? - What elements of the program are most successful? - What elements could be improved upon?		
Reply:	Very good - Employee awareness and compliance Procedures that are very specific rather than nebulas.		
Question 12:	Which programs do you perceive to be most successful in gaining active employee participation?		
Reply:	Safety and Security		
Question 13:	What tools (i.e. types of information, communication methods) do you need in order to build commitment? - Do you feel you have those necessary tools? - If not, what do you feel you might need?		
Reply:	Clear concise information, and rewards for compliance Yes		
Question 14:	If you were running the security awareness program at Hanford, what would you do to improve awareness and ownership?		
Reply:	Some sort of regular communications with employees. Rewards for successes		
Question 15:	How do you emphasize security awareness to your employees?		

	- What are some of the hassles you face in communicating security program information to your employees?
Reply:	Make it a subject of staff meetings and discuss problems as they arise
Question 16:	What frustrations do you have, if any, regarding employee compliance with the security awareness and ownership program guidelines? - How does that affect you as a manager?
Reply:	- Some sort of regular communications with employees. Rewards for successes We take the most conservative course
Question 17:	Do you think your employees have frustrations about security awareness and ownership? - If so, what are those frustrations related to?
Reply:	Yes disagreement in procedure interpretation
Question 18:	What are the consequences for failing to comply with security awareness and ownership program guidelines?
Reply:	Termination, poor performance ratings, or other penalties
Question 19:	What are your employees' perceptions about the problems with security awareness and ownership?
Reply:	- Don't see my employees with any problems accepting and following the rules. They cooperate and communicate very well in resolving any problems encountered.
Question 20:	What kinds of security awareness and ownership-related media have you seen? - Have you seen posters or calendars? - Have you seen computerized messages, such as animated banners? - Have you seen the Security Ed cartoons?
Reply:	Electronic mail updates Yes No
Question 21:	Do you have a preference as to which kinds of media you enjoy seeing?
Reply:	Electronic mail, documentaries and movies
Question 22:	Which of the security awareness and ownership materials are the most effective? Least effective? Why?
Reply:	
Question 23:	Is there something I haven't asked that you think is important for me to know?
Reply:	No
Question 24:	If there were one thing that could be done to increase employee ownership of security, what would it be?
Reply:	Weekly electronic mail updates
Question 25:	Who else should I talk to?
Reply:	Classified Document Control

A.23

Marketing Analysis and Strategy Formulation for Project Hanford Security Education and Awareness Program			
Interviewee:	Company:	Title:	Segment: Contr Mid. Lvl. Mgmt
Phone #	Loc:	Time @ Hanford:	Email:
Interviewer: Kevin Higginson	Date of Interview:		
Interview Summary			
Highlights of Interview			
Question 1:	Have you ever held a security clearance?		
Reply:	Yes (Q)		
Question 2:	What changes in security awareness and ownership requirements have you seen?		
Reply:	I have worked at many locations with varying degrees of security requirements. Over the past few years I have seen less security awareness. Because of the changing mission I would expect that to be the case. Application and awareness of training should be applied using the graded approach.		
Question 3:	How important is security awareness and ownership at Hanford?		
Reply:	Security awareness is very important for people to understand their responsibilities and what roles they play.		
Question 4:	Where, at Hanford, is security awareness and ownership most important? (Where should the program focus its energy?)		
Reply:	Areas which protect special interest, or that are vulnerable to sabotage.		
Question 5:	How important is security awareness and ownership in your area?		
Reply:	I think security is important in all levels of work here at Hanford. It is very important in the area I work in.		
Question 6:	What do you estimate your own awareness of security procedures and requirements to be? - What could be done to improve your awareness?		
Reply:	I am very aware. I have worked in many areas requiring a high level of knowledge.		
Question 7:	What elements of security awareness and ownership do you perceive to be of little value?		
Reply:	Bulletins on the intranet.		
Question 8:	What security awareness and ownership issues do you find to be most important?		
Reply:	Sabotage, fraud		
Question 9:	What other management priorities compete with managing security awareness and ownership requirements?		
Reply:	Production, Conduct of operations, training Low for my area Low for my area Positives are: Strong cost effective operation aligned to be successful toward meeting performance incentives agreed upon with the customer. Negatives are: Higher cost, slower production		
Question 10:	What are the criteria for having outstanding security awareness and ownership?		
Reply:	Controls, knowledge, and ownership		
Question 11:	How effective is the current program? - What elements of the program are most successful? - What elements could be improved upon?		
Reply:	Medium - Things enforced by patrol. Awareness		
Question 12:	Which programs do you perceive to be most successful in gaining active employee participation?		
Reply:	None		
Question 13:	What tools (i.e. types of information, communication methods) do you need in order to build commitment? - Do you feel you have those necessary tools? - If not, what do you feel you might need?		
Reply:	Understanding the requirements and committing to implementation no No We now perform safety meetings/topics at regular meeting. We could include safety topics for discussion as well.		
Question 14:	If you were running the security awareness program at Hanford, what would you do to improve awareness and ownership?		
Reply:	Strong communications to share requirements, lesson learned, and accept feedback		

Question 15:	How do you emphasize security awareness to your employees? - What are some of the hassles you face in communicating security program information to your employees?
Reply:	Discuss it as issues arise.
Question 16:	What frustrations do you have, if any, regarding employee compliance with the security awareness and ownership program guidelines? - How does that affect you as a manager?
Reply:	Understanding the requirements None
Question 17:	Do you think your employees have frustrations about security awareness and ownership? - If so, what are those frustrations related to?
Reply:	Insignificant
Question 18:	What are the consequences for failing to comply with security awareness and ownership program guidelines?
Reply:	Minor
Question 19:	What are your employees' perceptions about the problems with security awareness and ownership?
Reply:	Not understanding the rules
Question 20:	What kinds of security awareness and ownership-related media have you seen? - Have you seen posters or calendars? - Have you seen computerized messages, such as animated banners? - Have you seen the Security Ed cartoons?
Reply:	Computer messages No Yes
Question 21:	Do you have a preference as to which kinds of media you enjoy seeing?
Reply:	No
Question 22:	Which of the security awareness and ownership materials are the most effective? Least effective? Why?
Reply:	Banners are most effective. Posters are bad, they never change and no one looks at them.
Question 23:	Is there something I haven't asked that you think is important for me to know?
Reply:	No
Question 24:	If there were one thing that could be done to increase employee ownership of security, what would it be?
Reply:	Make it less cumbersome, easy and short.
Question 25:	Who else should I talk to?
Reply:	

A.24

Marketing Analysis and Strategy Formulation for Project Hanford Security Education and Awareness Program			
Interviewee:	Company:	Title:	Segment: Contr Mid. Lvl. Mgmt
Phone #	Loc:	Time @ Hanford:15yr	Email:
Interviewer: Kevin Higginson	Date of Interview:		
Interview Summary			
Highlights of Interview			
Question 1:	Have you ever held a security clearance?		
Reply:	Yes		
Question 2:	What changes in security awareness and ownership requirements have you seen?		
Reply:	Up and down		
Question 3:	How important is security awareness and ownership at Hanford?		
Reply:	Only second to safety		
Question 4:	Where, at Hanford, is security awareness and ownership most important? (Where should the program focus its energy?)		
Reply:	Where nuclear material is stored		
Question 5:	How important is security awareness and ownership in your area?		
Reply:	Top priority with safety		
Question 6:	What do you estimate your own awareness of security procedures and requirements to be? - What could be done to improve your awareness?		
Reply:	Very knowledgeable Training, short and frequently		
Question 7:	What elements of security awareness and ownership do you perceive to be of little value?		
Reply:	Don't know		
Question 8:	What security awareness and ownership issues do you find to be most important?		
Reply:	Disregard for procedures		
Question 9:	What other management priorities compete with managing security awareness and ownership requirements?		
Reply:	- As previously stated, security and safety are first in importance Security infraction penalties are significant		
Question 10:	What are the criteria for having outstanding security awareness and ownership?		
Reply:	Knowledge and constant awareness		
Question 11:	How effective is the current program? - What elements of the program are most successful? - What elements could be improved upon?		
Reply:	7 on 10 point scale Audits More frequent reminders		
Question 12:	Which programs do you perceive to be most successful in gaining active employee participation?		
Reply:	Short interactive reporting		
Question 13:	What tools (i.e. types of information, communication methods) do you need in order to build commitment? - Do you feel you have those necessary tools? - If not, what do you feel you might need?		
Reply:	Information and desire (motivation) Yes		
Question 14:	If you were running the security awareness program at Hanford, what would you do to improve awareness and ownership?		
Reply:	Mgmt cooperation to reward employee cooperation		
Question 15:	How do you emphasize security awareness to your employees? - What are some of the hassles you face in communicating security program information to your employees?		
Reply:			
Question 16:	What frustrations do you have, if any, regarding employee compliance with the security awareness and ownership program guidelines?		

	- How does that affect you as a manager?
Reply:	
Question 17:	Do you think your employees have frustrations about security awareness and ownership? - If so, what are those frustrations related to?
Reply:	Some employees at Hanford do Don't always know consequences of poor security to the nation
Question 18:	What are the consequences for failing to comply with security awareness and ownership program guidelines?
Reply:	Time off without pay or being fired
Question 19:	What are your employees' perceptions about the problems with security awareness and ownership?
Reply:	
Question 20:	What kinds of security awareness and ownership-related media have you seen? - Have you seen posters or calendars? - Have you seen computerized messages, such as animated banners? - Have you seen the Security Ed cartoons?
Reply:	Posters, signs, movies Yes no
Question 21:	Do you have a preference as to which kinds of media you enjoy seeing?
Reply:	No
Question 22:	Which of the security awareness and ownership materials are the most effective? Least effective? Why?
Reply:	Visual learning stays with you
Question 23:	Is there something I haven't asked that you think is important for me to know?
Reply:	No
Question 24:	If there were one thing that could be done to increase employee ownership of security, what would it be?
Reply:	Rewards for compliance
Question 25:	Who else should I talk to?
Reply:	

A.25

Marketing Analysis and Strategy Formulation for Project Hanford Security Education and Awareness Program			
Interviewee:	Company:	Title:	Segment: Contr Mid. Lvl. Mgmt
Phone #	Loc:	Time @ Hanford: 2yr	Email:
Interviewer: Sophia Orozco	Date of Interview:		
Interview Summary			
Highlights of Interview			
Question 1:	Have you ever held a security clearance?		
Reply:	Yes, a Q clearance at Ohio and Idaho, but not here.		
Question 2:	What changes in security awareness and ownership requirements have you seen?		
Reply:	Employees were more conscious at other labs than here but I worked in higher areas with more security. Here we rely on people. We find about 2 people per month, trying to enter our area without a badge. We even caught the guy who was doing a security check.		
Question 3:	How important is security awareness and ownership at Hanford?		
Reply:	It is important. People understand you can lose your job over it. Control of nuclear materials is high importance and well guarded. People know to watch for theft too. Its not very very important, but it is certainly important		
Question 4:	Where, at Hanford, is security awareness and ownership most important? (Where should the program focus its energy?)		
Reply:	Where there is special nuclear material or classified information.		
Question 5:	How important is security awareness and ownership in your area?		
Reply:	It is important as far as watching people walking around the facility. Being aware of strange events. Not at the same level as PFP though.		
Question 6:	What do you estimate your own awareness of security procedures and requirements to be? - What could be done to improve your awareness?		
Reply:	Pretty up on it. I read it all. I do the computer course, review procedures and changes and comment on revisions. It is a graded approach. -Increase awareness: HGET, security notices on email, and they can do semi-annual 30 min- 1hr. mandatory reviews.		
Question 7:	What elements of security awareness and ownership do you perceive to be of little value?		
Reply:	Can't think of any.		
Question 8:	What security awareness and ownership issues do you find to be most important?		
Reply:	For the 300-area access control of people, badges, anything related to special materials, and classified information. At a lesser level are things related to reporting of theft.		
Question 9:	What other management priorities compete with managing security awareness and ownership requirements?		
Reply:	<ul style="list-style-type: none"> - Day to day management, but it is a part of management to make sure they have the right attitude towards security. We have lots of meetings monthly. Emergency service reports in the morning many times deal with security and if I see a trend or a security incident I'll forward it to my managers. I will also forward control of nuclear material information. (approximately 3-4 forwards a week) I also talk to the staff about issues and help work things out. - Everything has negative consequences if its done well. In regard to security there are absolutely negative consequences. - I manage a safety group and push for safety issues, I don't know if anyone is pushing for security the same way. 		
Question 10:	What are the criteria for having outstanding security awareness and ownership?		
Reply:	Everyone knowing all the rules with positive and negative consequences and people being aware of any types of security incidents so that they can be aware.		
Question 11:	How effective is the current program? - What elements of the program are most successful? - What elements could be improved upon?		
Reply:	Reports are effective for him, but not everyone gets those. Most material has to do with safety and conduct. Successful = audits, those come up in meetings, proximity cards limiting entrances, and morning reports. Improve = I don't get information to enforce that security is important.		
Question 12:	Which programs do you perceive to be most successful in gaining active employee participation?		
Reply:	I don't see any. Someone came out and gave a talk once, that was very good.		
Question 13:	What tools (i.e. types of information, communication methods) do you need in order to build		

	<p>commitment?</p> <ul style="list-style-type: none"> - Do you feel you have those necessary tools? - If not, what do you feel you might need?
Reply:	If I had something that provided me a security topic and what I needed to do, I would do it. Every 2 weeks there is a staff meeting, this would make it easy for managers. And use audits.
Question 14:	If you were running the security awareness program at Hanford, what would you do to improve awareness and ownership?
Reply:	<ul style="list-style-type: none"> - A topical thing for managers or staff. - Take another look at HGET, make sure it includes the main points. Its been awhile sine I've taken it and I don't remember it so that the impression it left. - FAQs are pretty good. I would also check the list of sensitive countries to see if they are up to date and accurate. - In the 2420 building I see posters with various badges, these should be at the entrance of every facility. - Take another look at training for classifiers for clearance.
Question 15:	<p>How do you emphasize security awareness to your employees?</p> <ul style="list-style-type: none"> - What are some of the hassles you face in communicating security program information to your employees?
Reply:	Through staff meetings. None.
Question 16:	<p>What frustrations do you have, if any, regarding employee compliance with the security awareness and ownership program guidelines?</p> <ul style="list-style-type: none"> - How does that affect you as a manager?
Reply:	<p>Not really frustration, but people not actively looking for badges, or being aware.</p> <p>-If there were an increase in theft it could, if my employees were involved in an incident it would show up at appraisal time.</p>
Question 17:	<p>Do you think your employees have frustrations about security awareness and ownership?</p> <ul style="list-style-type: none"> - If so, what are those frustrations related to?
Reply:	No
Question 18:	What are the consequences for failing to comply with security awareness and ownership program guidelines?
Reply:	Disciplinary action that could lead to being dismissed.
Question 19:	What are your employees' perceptions about the problems with security awareness and ownership?
Reply:	None.
Question 20:	<p>What kinds of security awareness and ownership-related media have you seen?</p> <ul style="list-style-type: none"> - Have you seen posters or calendars? - Have you seen computerized messages, such as animated banners? - Have you seen the Security Ed cartoons?
Reply:	<p>Web page, posters, emergency morning reports, HGET, some e-mails.</p> <p>-Hasn't seen any calendars, but has seen the animated banners.</p>
Question 21:	Do you have a preference as to which kinds of media you enjoy seeing?
Reply:	Web pages
Question 22:	Which of the security awareness and ownership materials are the most effective? Least effective? Why?
Reply:	<p>Most = Managers expressing security at staff meetings. Posters if you change them, or the web page.</p> <p>Least = Posters that never change. They're like wallpaper, you don't notice them anymore.</p>
Question 23:	Is there something I haven't asked that you think is important for me to know?
Reply:	No
Question 24:	If there were one thing that could be done to increase employee ownership of security, what would it be?
Reply:	Signing a form with security expectations, an annual contract.
Question 25:	Who else should I talk to?
Reply:	Eric Bogt, director of various services was a manger at PFP

A.26

Marketing Analysis and Strategy Formulation for Project Hanford Security Education and Awareness Program			
Interviewee:	Company:	Title:	Segment: Contr Mid. Lvl. Mgmt
Phone #	Loc:	Time @ Hanford: 22yr	Email:
Interviewer: Sophia Orozco	Date of Interview:		
Interview Summary			
Highlights of Interview			
Question 1:	Have you ever held a security clearance?		
Reply:	I always have and still do. I had a Q while the plant was running, then I was downgraded. Where I work now I only need an L.		
Question 2:	What changes in security awareness and ownership requirements have you seen?		
Reply:	There used to be guards and metal detectors, more patrol now there is still a guard monitoring on all fuel locations, and you must hand geometry in.		
Question 3:	How important is security awareness and ownership at Hanford?		
Reply:	On a scale of 1-10 about and 8 or 9. It is important for safety and security. You can not have the wrong people coming in to sabotage or steal secrets.		
Question 4:	Where, at Hanford, is security awareness and ownership most important? (Where should the program focus its energy?)		
Reply:	FFTF secure area behind the double fence. PFP, K-basins, I'm not familiar with other areas as much		
Question 5:	How important is security awareness and ownership in your area?		
Reply:	I'm a maintenance manager. There are 20 to 22 people under me. All badge security is important so it is important for me to keep my employees aware of their responsibilities and roles.		
Question 6:	What do you estimate your own awareness of security procedures and requirements to be? - What could be done to improve your awareness?		
Reply:	Pretty good, I always check for strangers and I do not allow tailgating.		
Question 7:	What elements of security awareness and ownership do you perceive to be of little value?		
Reply:	None. Stealing fuel is not really as easy as they make it seem. They over kill that.		
Question 8:	What security awareness and ownership issues do you find to be most important?		
Reply:	There is adequate training and informing of issues.		
Question 9:	What other management priorities compete with managing security awareness and ownership requirements?		
Reply:	Getting the job done. -Required training. -I'm usually the last guy out so I make sure doors are locked. -Check for P on badge to "piggyback" in behind someone. ++Safety rewards for suggestions \$20-\$25 to correct problems. I think there is a Security Awareness award, but I can remember what it is. --Consequences are letters, reprimand, and discharge. These are real consequences I have seen them.		
Question 10:	What are the criteria for having outstanding security awareness and ownership?		
Reply:	Training, awareness, and examples. I try to show that I'm concerned to my employees through meetings. I receive stuff on "spy guy" Hanson and try to bring up things to look for.		
Question 11:	How effective is the current program? - What elements of the program are most successful? - What elements could be improved upon?		
Reply:	Pretty good. Successful= training and sharing information. No improvement suggestions.		
Question 12:	Which programs do you perceive to be most successful in gaining active employee participation?		
Reply:	Safety because employees are truly concerned. It makes everyone and their job better. They also have a very good turn around. Feedback and actions on suggestions. Security is probably the same way. They are friendly and fix things when needed.		
Question 13:	What tools (i.e. types of information, communication methods) do you need in order to build commitment? - Do you feel you have those necessary tools? - If not, what do you feel you might need?		
Reply:	What exists is adequate. I do monthly safety meetings that include some security issues.		
Question 14:	If you were running the security awareness program at Hanford, what would you do to improve awareness and		

	ownership?
Reply:	Heightening awareness is tough, but needs repetition. People get tired of it, but they'll remember. I would make sure everyone understands why security does what it does.
Question 15:	How do you emphasize security awareness to your employees? - What are some of the hassles you face in communicating security program information to your employees?
Reply:	Through meetings, and an exchange of information. No major hassles.
Question 16:	What frustrations do you have, if any, regarding employee compliance with the security awareness and ownership program guidelines? - How does that affect you as a manager?
Reply:	None, everyone knows the rules. -We lose a few tools once in awhile, I'd like to take care of that.
Question 17:	Do you think your employees have frustrations about security awareness and ownership? - If so, what are those frustrations related to?
Reply:	Yes, but they come to me and I find out why and explain it. One instance was the P on the badge. They did not understand it at first.
Question 18:	What are the consequences for failing to comply with security awareness and ownership program guidelines?
Reply:	Discipline. From verbal to time off to discharge. As a manager I have responsibilities and could face the same problems.
Question 19:	What are your employees' perceptions about the problems with security awareness and ownership?
Reply:	None. They question why all the guards, but they understand it's the way the job is done.
Question 20:	What kinds of security awareness and ownership-related media have you seen? - Have you seen posters or calendars? - Have you seen computerized messages, such as animated banners? - Have you seen the Security Ed cartoons?
Reply:	Posters, computer messages, and fliers. He prints his e-mails about security for employees. -Has seen banners but no calendars.
Question 21:	Do you have a preference as to which kinds of media you enjoy seeing?
Reply:	Computer messages, it is the most convenient.
Question 22:	Which of the security awareness and ownership materials are the most effective? Least effective? Why?
Reply:	Most is computer because of convenience. Least ??
Question 23:	Is there something I haven't asked that you think is important for me to know?
Reply:	?? They do so much already.
Question 24:	If there were one thing that could be done to increase employee ownership of security, what would it be?
Reply:	??
Question 25:	Who else should I talk to?
Reply:	Maurice Duffield

A.27

Marketing Analysis and Strategy Formulation for Project Hanford Security Education and Awareness Program			
Interviewee:	Company:	Title:	Segment: Contr Mid. Lvl. Mgmt
Phone #	Loc:	Time @ Hanford: 25yr	Email:
Interviewer: Sophia Orozco	Date of Interview:		
Interview Summary			
Highlights of Interview			
Question 1:	Have you ever held a security clearance?		
Reply:	Yes and I still do. I have always had a Q.		
Question 2:	What changes in security awareness and ownership requirements have you seen?		
Reply:	Security has changed to become more restrictive. As a result awareness has increased. Changes were done in polygraph testing, Psap programs, clearance/escort requirements , material surveillance requirements, length of clearance process.		
Question 3:	How important is security awareness and ownership at Hanford?		
Reply:	Extremely		
Question 4:	Where, at Hanford, is security awareness and ownership most important? (Where should the program focus its energy?)		
Reply:	PFP. This is the most vulnerable facility on sit		
Question 5:	How important is security awareness and ownership in your area?		
Reply:	I work at PFP		
Question 6:	What do you estimate your own awareness of security procedures and requirements to be? - What could be done to improve your awareness?		
Reply:	On a scale of 1-10 probably an 8. -better training on changes, more effective notification of changes -More consistent interpretation of requirements.		
Question 7:	What elements of security awareness and ownership do you perceive to be of little value?		
Reply:	None, it is very important.		
Question 8:	What security awareness and ownership issues do you find to be most important?		
Reply:	Access authorization and control.		
Question 9:	What other management priorities compete with managing security awareness and ownership requirements?		
Reply:	Production. It is on par with operations, safety and accountability.		
Question 10:	What are the criteria for having outstanding security awareness and ownership?		
Reply:	Good training, consistent documents, consistent interpretations, consistent enforcement of requirements. ARE CONSEQUENCES CONSISTENT RIGHT NOW?? No! but they should be.		
Question 11:	How effective is the current program? - What elements of the program are most successful? - What elements could be improved upon?		
Reply:	Moderately. Most = reach. To improve = I don't know what other opportunities are		
Question 12:	Which programs do you perceive to be most successful in gaining active employee participation?		
Reply:	Annual safety expo, Alara and Safety committees.		
Question 13:	What tools (i.e. types of information, communication methods) do you need in order to build commitment? - Do you feel you have those necessary tools? - If not, what do you feel you might need?		
Reply:	Simple concise, consistent information -No, we have voluminous procedures and polices that are difficult		
Question 14:	If you were running the security awareness program at Hanford, what would you do to improve awareness and ownership?		
Reply:	Run an interview like this. Reduce the current documentation into an easy form for the workers.		
Question 15:	How do you emphasize security awareness to your employees? - What are some of the hassles you face in communicating security program information to your employees?		
Reply:	Security is dealt with daily. I am constantly dealing with security people. It is built into the work. We routinely cover security issues and incidents. -Hassles: consistency in regulation or enforcement, consistent interpretation. This makes it difficult for people to		

	respect it when it is constantly changing and you never seem to get it right. You never seem to win.
Question 16:	What frustrations do you have, if any, regarding employee compliance with the security awareness and ownership program guidelines? - How does that affect you as a manager?
Reply:	Insufficient communication. -Miscommunication that leads to an incident, this stops processing until they recover.
Question 17:	Do you think your employees have frustrations about security awareness and ownership? - If so, what are those frustrations related to?
Reply:	I guarantee it. They are frustrated with security expectations, their inability to grasp and be aware of expectations. This is due to inconsistency and difficulty in understanding.
Question 18:	What are the consequences for failing to comply with security awareness and ownership program guidelines?
Reply:	Security stops operations. When there are incidents reported, clearance gets pulled, it takes management time, and people can get relocated or go through programs to get reinstated.
Question 19:	What are your employees' perceptions about the problems with security awareness and ownership?
Reply:	I would guess training and understanding.
Question 20:	What kinds of security awareness and ownership-related media have you seen? - Have you seen posters or calendars? - Have you seen computerized messages, such as animated banners? - Have you seen the Security Ed cartoons?
Reply:	Bulletin board, reach, fliers, posters, I read policies and procedures. -no calendars seen but has seen some security things on the internet.
Question 21:	Do you have a preference as to which kinds of media you enjoy seeing?
Reply:	No not really.
Question 22:	Which of the security awareness and ownership materials are the most effective? Least effective? Why?
Reply:	Most = period refresher training like HGET but its not very intensive for the requirements at PFP. Least = Posters. They are on a cork board with lots of other stuff. People do not look at them.
Question 23:	Is there something I haven't asked that you think is important for me to know?
Reply:	No
Question 24:	If there were one thing that could be done to increase employee ownership of security, what would it be?
Reply:	Simplify documentation so its easier to understand and build awareness from
Question 25:	Who else should I talk to?
Reply:	Bill F Russell, PFP coordinator with security entities.

A.28

Marketing Analysis and Strategy Formulation for Project Hanford Security Education and Awareness Program			
Interviewee:	Company:	Title:	Segment: Contr Mid. Lvl. Mgmt
Phone #	Loc:	Time @ Hanford: 8yr	Email:
Interviewer: Sophia Orozco	Date of Interview:		
Interview Summary			
Highlights of Interview			
Question 1:	Have you ever held a security clearance?		
Reply:	I've had an L clearance for the last 3- years.		
Question 2:	What changes in security awareness and ownership requirements have you seen?		
Reply:	From little to very high to now about the medium level. These changes have occurred because of what the work being done.		
Question 3:	How important is security awareness and ownership at Hanford?		
Reply:	Pretty important. Some areas very others not significant. It is based on the hazards.		
Question 4:	Where, at Hanford, is security awareness and ownership most important? (Where should the program focus its energy?)		
Reply:	Where the fuel is. Where higher risk is, and where hazards can potentially hurt people.		
Question 5:	How important is security awareness and ownership in your area?		
Reply:	Medium		
Question 6:	What do you estimate your own awareness of security procedures and requirements to be? - What could be done to improve your awareness?		
Reply:	Fairly good. I don't know what else they could do. I do not know as much as some others, but I do not need to.		
Question 7:	What elements of security awareness and ownership do you perceive to be of little value?		
Reply:	All of it is valuable.		
Question 8:	What security awareness and ownership issues do you find to be most important?		
Reply:	HGET material and awareness of badges is most important.		
Question 9:	What other management priorities compete with managing security awareness and ownership requirements?		
Reply:	Security is only about .5% of what I do. Everything competes. The positive of security is good awareness so it is always considered. The security aspect doesn't impact us much. There are consequences in the security department. It is like other programs just not as visible, publicized, not as intrusive (so many requirements.)		
Question 10:	What are the criteria for having outstanding security awareness and ownership?		
Reply:	I'm not sure if posters are really effective reminders. Security doesn't impact much so it is possible to have a good program with out visibility.		
Question 11:	How effective is the current program? - What elements of the program are most successful? - What elements could be improved upon?		
Reply:	Very good. I have confidence in key control and in responsiveness if needed. No improvement suggestions.		
Question 12:	Which programs do you perceive to be most successful in gaining active employee participation?		
Reply:	Wearing badges and keeping patrols active.		
Question 13:	What tools (i.e. types of information, communication methods) do you need in order to build commitment? - Do you feel you have those necessary tools? - If not, what do you feel you might need?		
Reply:	I think it is the right level with good people. I have had good experience with them, leave it the same.		
Question 14:	If you were running the security awareness program at Hanford, what would you do to improve awareness and ownership?		
Reply:	?		
Question 15:	How do you emphasize security awareness to your employees? - What are some of the hassles you face in communicating security program information to your employees?		
Reply:	Had security come out with their dogs, set expectations, emphasize importance, and use lessons learned. No hassles.		
Question 16:	What frustrations do you have, if any, regarding employee compliance with the security awareness and ownership		

	<p>program guidelines?</p> <ul style="list-style-type: none"> - How does that affect you as a manager?
Reply:	No, they've accepted and adhere to what is required. Yes, I'd have to deal with it and it would reflect badly on me, maybe even effect if I'd be working here.
Question 17:	<p>Do you think your employees have frustrations about security awareness and ownership?</p> <ul style="list-style-type: none"> - If so, what are those frustrations related to?
Reply:	No, we did when it was high security but not any more.
Question 18:	What are the consequences for failing to comply with security awareness and ownership program guidelines?
Reply:	Reviews to losing your job.
Question 19:	What are your employees' perceptions about the problems with security awareness and ownership?
Reply:	They don't feel like they have options so they just live with it. They feel security is there is they need them.
Question 20:	<p>What kinds of security awareness and ownership-related media have you seen?</p> <ul style="list-style-type: none"> - Have you seen posters or calendars? - Have you seen computerized messages, such as animated banners? - Have you seen the Security Ed cartoons?
Reply:	Posters, signs on badges, verbiage in procedures, HGET training. Has seen calendars, but not in his building, and also has seen computer messages and banners.
Question 21:	Do you have a preference as to which kinds of media you enjoy seeing?
Reply:	No
Question 22:	Which of the security awareness and ownership materials are the most effective? Least effective? Why?
Reply:	<p>Most = posters at first, but they need to change them. So, lessons learned because they apply and take a personal view.</p> <p>Least = banners because I could not recall seeing them.</p>
Question 23:	Is there something I haven't asked that you think is important for me to know?
Reply:	No
Question 24:	If there were one thing that could be done to increase employee ownership of security, what would it be?
Reply:	I think it is the right level with good people. I have had good experience with them, leave it the same.
Question 25:	Who else should I talk to?
Reply:	

A.29

Marketing Analysis and Strategy Formulation for Project Hanford Security Education and Awareness Program			
Interviewee:	Company:	Title:	Segment: Contr Mid. Lvl. Mgmt
Phone #	Loc:	Time @ Hanford: 20yr	Email:
Interviewer: Sophia Orozco	Date of Interview:		
Interview Summary			
Highlights of Interview			
Question 1:	Have you ever held a security clearance?		
Reply:	Yes, but I don't anymore.		
Question 2:	What changes in security awareness and ownership requirements have you seen?		
Reply:	10 years ago the reduction of clearances. Everyone used to have one then it went to those who just needed it. This was a good change.		
Question 3:	How important is security awareness and ownership at Hanford?		
Reply:	Very important.		
Question 4:	Where, at Hanford, is security awareness and ownership most important? (Where should the program focus its energy?)		
Reply:	In the protected areas.		
Question 5:	How important is security awareness and ownership in your area?		
Reply:	Its important for some business information that we have, but not as much.		
Question 6:	What do you estimate your own awareness of security procedures and requirements to be? - What could be done to improve your awareness?		
Reply:	On a 1-10 scale about an 8-9. I read the reach articles, and I know all the concepts but not detail. That increases with being involved in events.		
Question 7:	What elements of security awareness and ownership do you perceive to be of little value?		
Reply:	How much they stress that contractors in town have to have the same clearance as everyone else even if they are not in a high security area, it shouldn't be that way.		
Question 8:	What security awareness and ownership issues do you find to be most important?		
Reply:	Protection of classified information and special material.		
Question 9:	What other management priorities compete with managing security awareness and ownership requirements?		
Reply:	A lot. Performance budgets. Security does not fit in real high. Periodically in weekly meetings we review security issues, but Performance and budget get priority. I see negative consequences for security. Some can loose their badge or clearance, I've seen this, but I've never seen anyone lose their job.		
Question 10:	What are the criteria for having outstanding security awareness and ownership?		
Reply:	That all employees understand it and are aware of it.		
Question 11:	How effective is the current program? - What elements of the program are most successful? - What elements could be improved upon?		
Reply:	?		
Question 12:	Which programs do you perceive to be most successful in gaining active employee participation?		
Reply:	Reach. I don't see them doing much very actively. There is little communication.		
Question 13:	What tools (i.e. types of information, communication methods) do you need in order to build commitment? - Do you feel you have those necessary tools? - If not, what do you feel you might need?		
Reply:	Clear, easy to understand guides and procedures. Show that security is concerned about others needs not just their own.		
Question 14:	If you were running the security awareness program at Hanford, what would you do to improve awareness and ownership?		
Reply:	Have security folks get out and understand the different businesses before requiring more procedures.		
Question 15:	How do you emphasize security awareness to your employees? - What are some of the hassles you face in communicating security program information to your employees?		
Reply:	Review procedures and make sure they understand them and know that's the way we do business. No hassles		
Question 16:	What frustrations do you have, if any, regarding employee compliance with the security awareness and ownership program guidelines?		

	- How does that affect you as a manager?
Reply:	Sometimes people feel the security guidelines don't make any sense or apply to their area. Why apply everything the same across the board? If employees don't comply then I have to deal with them. Effects annual appraisals of employee but does not particularly effect mine.
Question 17:	Do you think your employees have frustrations about security awareness and ownership? - If so, what are those frustrations related to?
Reply:	See 16
Question 18:	What are the consequences for failing to comply with security awareness and ownership program guidelines?
Reply:	Depends on the extent and nature. Moderate will get just a talk but serious is totally different.
Question 19:	What are your employees' perceptions about the problems with security awareness and ownership?
Reply:	Frustrations have been there for a long time and security doesn't care. They're focused on their aspect
Question 20:	What kinds of security awareness and ownership-related media have you seen? - Have you seen posters or calendars? - Have you seen computerized messages, such as animated banners? - Have you seen the Security Ed cartoons?
Reply:	Reach articles, occasionally in the Hanford today, I've seen a poster or two. No computer stuff or calendars.
Question 21:	Do you have a preference as to which kinds of media you enjoy seeing?
Reply:	No, I think you have to use all of them and vary them so people don't get numb to them. I just read reach.
Question 22:	Which of the security awareness and ownership materials are the most effective? Least effective? Why?
Reply:	Most = well written reach article. Least = e-mails, they get ignored
Question 23:	Is there something I haven't asked that you think is important for me to know?
Reply:	No
Question 24:	If there were one thing that could be done to increase employee ownership of security, what would it be?
Reply:	Communications program so everyone understands that security can be a part of their job, not contradictory or in conflict with it.
Question 25:	Who else should I talk to?
Reply:	

A.30

Marketing Analysis and Strategy Formulation for Project Hanford Security Education and Awareness Program			
Interviewee:	Company:	Title:	Segment: Contr Mid. Lvl. Mgmt
Phone #	Loc:	Time @ Hanford: 19yr	Email:
Interviewer: Sophia Orozco	Date of Interview:		
Interview Summary			
Highlights of Interview			
Question 1:	Have you ever held a security clearance?		
Reply:	Yes. I held a clearance until 1997 then I changed jobs and did not need it anymore		
Question 2:	What changes in security awareness and ownership requirements have you seen?		
Reply:	<ul style="list-style-type: none"> - Plutonium Finishing Plant PFP has been getting stricter due to increased security technology. In the past they used to search every car, methods were not as technologically advanced. - In 1982 there was easier access to certain parts, then in 1984 the processing of plutonium began again and it became strict. - Now there are sensitive metal detectors. The cold war is over, but now we are worried about terrorism. - It has become more and more restricted, more needed for clearance, but just for PFP. The rest of the Hanford site security is decreasing, its not patrolled like it used to be. 		
Question 3:	How important is security awareness and ownership at Hanford?		
Reply:	Highly, where nuclear weapons (plutonium) is stored it's a question of national security. For the rest of Hanford there is more concern with personal property and information on the business aspect.		
Question 4:	Where, at Hanford, is security awareness and ownership most important? (Where should the program focus its energy?)		
Reply:	Within the nuclear protection program		
Question 5:	How important is security awareness and ownership in your area?		
Reply:	I'm in the 324 building. Here sabotage is a threat. There are hot cells out there. High radiation is potentially harmful to employees and there is high cleanup costs, but we don't deal with classification material.		
Question 6:	What do you estimate your own awareness of security procedures and requirements to be?		
Reply:	<ul style="list-style-type: none"> - What could be done to improve your awareness? - On a 1-10 scale an 8, or fairly high. I know my responsibilities and I am aware of programs because I used to help fund them. I am a cost accounting manager for the facility. Security used to get monies from all programs but now the government funds them and other programs receive less to cover their costs. - Drill me more often. Offer all plant meetings that cover general topics. Require monthly safety meetings, improvement plans, and project goals. - Chet has given these presentations and my group liked it. He did a home security talk. Do more of these with different topics. - Improve training. Through the computer based training, people click through everything. Its easy to get by with out learning much. You can take the test without reading any information. Move a little away from computer based and find a happy medium. 		
Question 7:	What elements of security awareness and ownership do you perceive to be of little value?		
Reply:	<ul style="list-style-type: none"> - Changing of passwords. It makes it hard to remember. I see no value in it, it just forces people to write it down which they really do not want. - Security seems transparent. Once in awhile a guard comes to check badges...I hate having to take my badge out of the plastic holder. 		
Question 8:	What security awareness and ownership issues do you find to be most important?		
Reply:	Personal employee badge checks because it's the first line of defense since there are no more barricades or guards.		
Question 9:	What other management priorities compete with managing security awareness and ownership requirements?		
Reply:	<ul style="list-style-type: none"> - Everything. Security is transparent. We don't fund it anymore. Security issues are dealt with at the higher level for budget reasons. All I do is have employees buy donuts if they forget their badge. - The risk-based decision that takes priority is clean up because we are so close to the river. Weighing the risk and trying to balance takes time. <p>Safety is high because there is no war threat. You can therefore take time to be safe. Security is somewhat tied with safety.</p>		
Question 10:	What are the criteria for having outstanding security awareness and ownership?		
Reply:	An aware work force.		
Question 11:	How effective is the current program?		
Reply:	<ul style="list-style-type: none"> - What elements of the program are most successful? - What elements could be improved upon? <p>HGET computer based is an annoyance and not effective.</p>		

	Presence and people being questioned. Guards do this. They are a necessary evil. You have to be patrolled. Random searches serve as a deterrent.
Question 12:	Which programs do you perceive to be most successful in gaining active employee participation?
Reply:	Being stopped and asked for badge. Special interest training
Question 13:	What tools (i.e. types of information, communication methods) do you need in order to build commitment? - Do you feel you have those necessary tools? - If not, what do you feel you might need?
Reply:	Knowledge of what is available to him from the security dept. What is out there, what does Chet have that will help him as a manager.
Question 14:	If you were running the security awareness program at Hanford, what would you do to improve awareness and ownership?
Reply:	Get out amongst the people. I would be an evangelistic preacher. Ask to give presentations to groups. You are trying to sell something, the best way to do that is face to face.
Question 15:	How do you emphasize security awareness to your employees? - What are some of the hassles you face in communicating security program information to your employees?
Reply:	Employees who forget their badge must bring donuts. I also sit with employees at least once a year and go through the standards of conduct and it has several points about security so they can be aware of what is required of them. No hassles
Question 16:	What frustrations do you have, if any, regarding employee compliance with the security awareness and ownership program guidelines? - How does that affect you as a manager?
Reply:	I have a compliant staff. If not compliant as a manager I would have to take action according to the standards.
Question 17:	Do you think your employees have frustrations about security awareness and ownership? - If so, what are those frustrations related to?
Reply:	Taking their badge out of the plastic. They also complain about being the one that is randomly checked. This is not something I think needs to be changed however. It is necessary.
Question 18:	What are the consequences for failing to comply with security awareness and ownership program guidelines?
Reply:	See the PHMC conduct sheet. All subject for review. A manager is equally guilty if he is aware. On the extreme it could result in termination
Question 19:	What are your employees' perceptions about the problems with security awareness and ownership?
Reply:	Not aware of any.
Question 20:	What kinds of security awareness and ownership-related media have you seen? - Have you seen posters or calendars? - Have you seen computerized messages, such as animated banners? - Have you seen the Security Ed cartoons?
Reply:	- Chets presentation, HGET annual refresher, log on security page, general employee messages by e-mail, signs on the road, posters. - Has not seen calendars, mouse pads, or animated banners.
Question 21:	Do you have a preference as to which kinds of media you enjoy seeing?
Reply:	I like one on one. Presentations.
Question 22:	Which of the security awareness and ownership materials are the most effective? Least effective? Why?
Reply:	?
Question 23:	Is there something I haven't asked that you think is important for me to know?
Reply:	No
Question 24:	If there were one thing that could be done to increase employee ownership of security, what would it be?
Reply:	Encourage Chet to get info out on what is available. If it is easy and in his hands he would do it.
Question 25:	Who else should I talk to?
Reply:	Ray Stevens, Daryle Riffe, and Mick Talbot.

A.31

Marketing Analysis and Strategy Formulation for Project Hanford Security Education and Awareness Program			
Interviewee:	Company:	Title:	Segment: Contr Mid. Lvl. Mgmt
Phone #	Loc:	Time @ Hanford: 23 yr	Email:
Interviewer: Sophia Orozco	Date of Interview:		
Interview Summary			
Highlights of Interview			
Question 1:	Have you ever held a security clearance?		
Reply:			
Question 2:	What changes in security awareness and ownership requirements have you seen?		
Reply:	There has absolutely been a change. It is not emphasized as much overall, but it is emphasized more in some areas. The change occurred years ago, in the mid to late 80s when production closed and clean up started. Before this most people were involved in highly secure areas, but now that's not true. When security was taken away it was like a slap in the face, there were feelings of mistrust. This made like a caste system and took status away. Requirements to get clearances became more rigid. This was a decision by management not by employees. New people seem less aware of security and only seem to see the badge as important.		
Question 3:	How important is security awareness and ownership at Hanford?		
Reply:	If you are in a security clearance area, it is very important.		
Question 4:	Where, at Hanford, is security awareness and ownership most important? (Where should the program focus its energy?)		
Reply:	Where there is Plutonium		
Question 5:	How important is security awareness and ownership in your area?		
Reply:	It is important when dealing with sensitive and confidential information		
Question 6:	What do you estimate your own awareness of security procedures and requirements to be? - What could be done to improve your awareness?		
Reply:	I know the requirements, not detailed though. If I need information I will look on the Internet or call someone. - There is not much they can do to improve my awareness. People learn by doing, so maybe you could test me more.		
Question 7:	What elements of security awareness and ownership do you perceive to be of little value?		
Reply:	- All elements have some value, most people do not get all of the security information so what they get is of value.		
Question 8:	What security awareness and ownership issues do you find to be most important?		
Reply:	Each individual is to be responsible for ensuring that people are appropriately badged and are in areas appropriate for them.		
Question 9:	What other management priorities compete with managing security awareness and ownership requirements?		
Reply:	I don't communicate about security. We only have the rule that if someone forgets his/her badge then they have to bring donuts. They get what they need through employee training. We only communicate safety by doing evaluations; this has personal impact on performance appraisals. Security is not seen as part of environment, safety or health.		
Question 10:	What are the criteria for having outstanding security awareness and ownership?		
Reply:	Give people an understanding of their responsibilities and consequences. There are only consequences for large problems right now.		
Question 11:	How effective is the current program? - What elements of the program are most successful? - What elements could be improved upon?		
Reply:	The graded approach is effective. It reaches who it needs to reach, and gives clearance training when needed.		
Question 12:	Which programs do you perceive to be most successful in gaining active employee participation?		
Reply:	Reward programs have the biggest participation. I can't think of security doing this off hand. Safety does a crossword puzzle giving the 1 st few to complete it a prize. They also have a monthly slogan contest.		
Question 13:	What tools (i.e. types of information, communication methods) do you need in order to build commitment? - Do you feel you have those necessary tools? - If not, what do you feel you might need?		
Reply:	Access to people. This is easily done with computers: HGET and e-mails heighten awareness.		
Question 14:	If you were running the security awareness program at Hanford, what would you do to improve awareness and ownership?		
Reply:	More bulletins, but for all employees.		

Question 15:	How do you emphasize security awareness to your employees? - What are some of the hassles you face in communicating security program information to your employees?
Reply:	They need to bring donuts if they forget their badge.
Question 16:	What frustrations do you have, if any, regarding employee compliance with the security awareness and ownership program guidelines? - How does that affect you as a manager?
Reply:	It is frustrating when the guards say that the badge cannot be in a plastic holder. It has to be handed to them.
Question 17:	Do you think your employees have frustrations about security awareness and ownership? - If so, what are those frustrations related to?
Reply:	No one has mentioned any.
Question 18:	What are the consequences for failing to comply with security awareness and ownership program guidelines?
Reply:	It depends on the magnitude. Rules are rules; sometimes it would mean grounds for dismissal. Individuals are responsible for their own actions; a manager can only guide them.
Question 19:	What are your employees' perceptions about the problems with security awareness and ownership?
Reply:	None
Question 20:	What kinds of security awareness and ownership-related media have you seen? - Have you seen posters or calendars? - Have you seen computerized messages, such as animated banners? - Have you seen the Security Ed cartoons?
Reply:	- Unaided recall: badges, signs on side of road, billboards, Reach cartoon. - Aided recall: Hasn't seen any posters lately...as an after thought remembered seeing posters in elevators, thought this was strange because 1 st floor employees won't get to see them. Had not seen any computer messages.
Question 21:	Do you have a preference as to which kinds of media you enjoy seeing?
Reply:	Some animation, but not memos
Question 22:	Which of the security awareness and ownership materials are the most effective? Least effective? Why?
Reply:	Most = Classroom and HGET training if it is required Least= Emails and Reach because you don't have to pay attention to them.
Question 23:	Is there something I haven't asked that you think is important for me to know?
Reply:	No
Question 24:	If there were one thing that could be done to increase employee ownership of security, what would it be?
Reply:	It is asinine to have to take my badge out of its plastic.
Question 25:	Who else should I talk to?
Reply:	



PHMC Standards of Conduct

There are regulations that govern our conduct as employees just as there are regulations governing us as citizens in the communities in which we live. These regulations are intended to keep our Company a safe, pleasant, productive, and desirable place to work. They are for your information and to assure fair administration of disciplinary action if it is ever necessary. All employees are expected to abide by these Standards of Conduct. (Refer to HNF-PRO-033, *Employee Discipline*)

While it is not practical to list every act of misconduct which might require disciplinary action, the following provides a basic pattern for such action:

A. EXTREMELY SERIOUS MISCONDUCT

Any of the following types of actions are considered extremely serious misconduct and may result in immediate discharge.

1. Deliberate disregard of safety rules and safety procedures.
2. Insubordination, including failure to carry out definite instructions or assignments.
3. Taking or receiving, without authorization, property belonging to the Company, fellow employees, a contractor, a vendor, the government, or others.
4. Deliberate misuse of or damage to Company property, government property, or the property of another employee.
5. Falsification of records or reports.
6. Violations of any criminal or civil law, on or off Company/government property, which could likely have an impact on the employment relationship, the workplace, or the image/reputation of the Company and/or the customer.
7. Possessing, passing, using, or threatening to use weapons, incendiary devices, or explosives, or conspiring to take such action when not a part of assigned duties.
8. Security violations which jeopardize the proper control of Company property or information.
9. Fighting, assaulting, or other disorderly conduct, such as the use of abusive or threatening language.
10. Sleeping during working time.
11. Immoral or obscene conduct.
12. Deliberate interference with experiments, tests, or operations.
13. Organizing, operating, or conducting gambling activities.
14. Inciting to riot.
15. Unauthorized disclosure, use, or disposition of Company or government records.

(Over)

16. Using, possessing, passing (or conspiring to use, possess, or pass), or being under the influence of any intoxicants, narcotics, hallucinogenics, depressants, stimulants, or other such drugs anywhere on the Hanford Site or at any Company or government location.
17. Concealing defective work.
18. Engaging in illegal or unethical business practices or creating, maintaining, and/or failing to disclose a conflict with the business interests of the company or the U.S. Government.
19. An unreported absence of 3 consecutive working days.

B. SERIOUS MISCONDUCT

The following types of actions are considered serious misconduct. The first infraction may result in at least a three-day suspension without pay. A second infraction, not necessarily of the same type, may result in discharge.

1. Violation of safety rules and safety practices or failure to use or wear designated safety equipment.
2. Careless waste of materials or abuse of tools and equipment.
3. Producing defective work through carelessness or negligence.
4. Playing pranks or "horseplay," or causing a disruption in the workplace through gesture, verbal comments, or written or electronic communication.
5. Failure to follow operations or other procedures.

C. MISCONDUCT

The following types of actions are considered misconduct. The first infraction may result in a written warning. A second infraction, not necessarily of the same type, may result in at least a three-day suspension without pay. A third infraction, not necessarily of the same type, may result in suspension without pay, subject to discharge.

1. Failure to report a personal injury to the supervisor or the Health Service Center on the day it occurs.
2. Absence from the work area without permission or satisfactory reason for leaving the job or work area before the lunch period or at the end of a shift.
3. Excessive absences or tardiness, unreported absence, or absence/tardiness without justifiable cause.
4. Posting unauthorized notices, defacing Company or government property, or tampering with Company bulletin boards.
5. Improper parking or operation of vehicles on Company or government property.
6. Security infractions.

06/11/99

Appendix B

Security Education - Special Interest Group Interviews

Marketing Analysis and Strategy Formulation for Project Hanford Security Education and Awareness Program			
Interviewee:	Company:	Title:	Segment: TRADE Security Representative
Phone #	Loc: Arlington, VA		
Interviewer: Alison Mareum	Date of Interview:		SE SIG Conference Interview
Interview Summary			
Highlights of Interview			
Question 1:	Where are you from? What is your position? How long have you been there?		
Reply:	DOE headquarters Program Manager for tech and OPSEC Has been there nearly eleven years, was a contractor the previous seven years		
Question 2:	How is security important to your work/company?		
Reply:	Writes policy for protection of classified information as my job to provide direction for others.		
Question 3:	What precautions are taken at the end of the workday?		
Reply:	Follow a checklist that rotates. Safes, desks, phones, and computers approved for classifieds, shut/lock doors. Who ever is responsible for completing the checklist signs off on the list.		
Question 4:	How so you build security awareness? (How is it promoted?)		
Reply:	Through marketing. We use examples that people can relate to. There are two ways: personal and corporate (Senior manager ownership). Also, through constant daily reminders such as pens, posters newspaper articles, etc		
Question 5:	What approaches are most effective? Why? Which are least effective? Why?		
Reply:	Most effective: Local themes because they are tied to the facility rather than the country. Short messages on computers at log on are good too. Also, posters but it is important to change them, perhaps monthly. Least effective: When media is not in plain English; hidden messages or too much information that causes Absorption problems.		
Question 6:	Have employees ever been involved in the process of developing security programs and/or guidelines? -If so, how was this done? Was this a successful approach? If not, do you feel it could encourage employee participation/ownership? -how could this approach be implemented?		
Reply:	Including employees in policies and procedures has been successful because it helps them understand difficult issues and policies.		
Question 7:	I know that requiring badges to be worn is a common practice at DOE facilities; is this true for your area? What are the consequences for failing to wear a badge? Is this a common problem?		
Reply:	The only badge problem is they look different. A couple years ago I tried to make badges look the same: to decrease discrimination but this did not work. There needs to be a clear distinction to recognize what the badge is for.		
Question 8:	Are there any plans for future promotion of security awareness in- progress? Is there anything you would like to try but have not been able to thus far?		
Reply:	For the future use computer based training as annual refresher s concerning updated policies, and more use of web based training. I'm not aware of any ideas we have not been able to do.		

Marketing Analysis and Strategy Formulation for Project Hanford Security Education and Awareness Program			
Interviewee:	Company:	Title:	Segment: TRADE Security Representative
Phone #	Loc: Arlington, VA		
Interviewer: Sophia Orozco	Date of Interview:		SE SIG Conference Interview
Interview Summary			
Highlights of Interview This is an interview conducted with two interviewees simultaneously at their request. Both are from the same location and had the same perspectives.			
Question 1:	Where are you from? What is your position? How long have you been there?		
Reply:	Rocky Flats 1. Site Coordinator and Team Lead - 11 years 2. Security Education Specialist - 5 1/2 years		
Question 2:	How is security important to your work/company?		
Reply:	We are responsible for making sure employees are adhering to security responsibilities and site requirements.		
Question 3:	What precautions are taken at the end of the workday?		
Reply:	Locking-up		
Question 4:	How so you build security awareness? (How is it promoted?)		
Reply:	Through security briefings, videos, developing posters, articles, brochures, web-based training, web sites, and weekly publications (newsletters). We develop training for other companies on numerous aspects. Our goals are to make training specific to them, explain the why, and tell where it is written for guidance.		
Question 5:	What approaches are most effective? Why Which are least effective? Why?		
Reply:	Most effective: one-on-one training and web training. Least effective: read and sign.		
Question 6:	Have employees ever been involved in the process of developing security programs and/or guidelines? -If so, how was this done? Was this a successful approach? If not, do you feel it could encourage employee participation/ownership? -how could this approach be implemented?		
Reply:	We do this by basing training on incidents known, having knowledge assessments, and giving an opportunity for evaluations after briefings. This is successful because we get a lot of useful feedback.		
Question 7:	I know that requiring badges to be worn is a common practice at DOE facilities; is this true for your area? What are the consequences for failing to wear a badge? Is this a common problem?		
Reply:	This is true. The consequence would include being escorted by a guard off of the facility. This is not necessarily a common problem but security infractions are possible.		
Question 8:	Are there any plans for future promotion of security awareness in- progress? Is there anything you would like to try but have not been able to thus far?		
Reply:	Future plans would include refresher briefings with themes that will get attention. But this is hard to do without focus from top management. One idea is a car show. Display nice cars and explain that "you protect your car, why not security?" Another idea is to change computer-based training to a game show format. Use "AI Moral."		

Marketing Analysis and Strategy Formulation for Project Hanford Security Education and Awareness Program			
Interviewee:	Company:	Title:	Segment: TRADE Security Representative
Phone #	Loc: Arlington, VA		
Interviewer: Sophia Orozco	Date of Interview:		SE SIG Conference Interview
Interview Summary			
Highlights of Interview			
Question 1:	Where are you from? What is your position? How long have you been there?		
Reply:	DOE headquarters Classification Officer of Security 33 years		
Question 2:	How is security important to your work/company?		
Reply:	National Security Interest		
Question 3:	What precautions are taken at the end of the workday?		
Reply:	Classified documents are locked in safes, classified parts (weapon components) are locked in vaulted warehouses. We have twenty-four hours, seven days a week security including a military professional force team.		
Question 4:	How so you build security awareness? (How is it promoted?)		
Reply:	To build the program, first, a DOE order requirement needs to be converted to a general plant requirement. To build awareness we currently have people working with people, presentations and going to different departments and organizations to address security issues.		
Question 5:	What approaches are most effective? Why? Which are least effective? Why?		
Reply:	Most effective: person to person because it builds a relationship and offers instant feedback. Least effective: read and sign, because people don't read, they just sign.		
Question 6:	Have employees ever been involved in the process of developing security programs and/or guidelines? -If so, how was this done? Was this a successful approach? If not, do you feel it could encourage employee participation/ownership? -how could this approach be implemented?		
Reply:	Yes, every day. Suggestions are heard every day especially in meetings. We will then either implement or give the reason why idea wasn't done if we can't. This has been successful.		
Question 7:	I know that requiring badges to be worn is a common practice at DOE facilities; is this true for your area? What are the consequences for failing to wear a badge? Is this a common problem?		
Reply:	Consequences would be removal from the plant site, a guard would remove them. But we don't have that issue because you can't get into the area without a badge.		
Question 8:	Are there any plans for future promotion of security awareness in- progress? Is there anything you would like to try but have not been able to thus far?		
Reply:	We always have future plans; right now it is to have inclusion of security awareness through ISSM to make high visibility with in DOE. No, we've been able to do everything that we've wanted.		
Additional Question:	Can you explain why it is necessary to require employees to take their badge out of its plastic holder?		
Reply:	We have guards everywhere; they are required to take the badge out of the plastic for reasons I can not go into. They need to better see and touch the badge.		

Appendix C

A Case Study of Safety and Security Programs

This case study reviews the similarities and differences between the approach and deployment of security awareness and the DOE safety and health program from the late 1980's through the present. This review is primarily a generic comparison of the programs across the DOE complex although there are some specific references to programs at Hanford.

The description of the programs and their evolution that are presented in the table reflect the perceptions of the six DOE security and safety experts identified in Table C.1.

Table C.1

Security and Safety experts consulted in personal communication	
A. DOE-RL Mgr	DOE-Richland Operations Office
B. Michael Hillman	DOE-Headquarters (EH)
Barry Cooksey	DOE-Headquarters (OA)
Jim Schildknecht	Fluor Daniels, Performance Support
Obie Amacker	Pacific Northwest National Laboratory, Manager, Safeguards and Security Services
Jan Jaeger	Pacific Northwest National Laboratory, Manager, Independent Oversight

Table C. 2

Changing Perceptions of Need for Protection – Late 1980s to Present	
Security Awareness	Safety and Health
<ol style="list-style-type: none"> 1. In the late 1980s, the security awareness program had the largest market share (priority) of all of the protection programs. The mission and security were both higher priorities than worker safety and health. 2. The need for security discipline was understood, accepted, and generally complied with in the late 1980's. 3. Priority, funding, and clarity of need for security awareness diminished during the 1990s. 4. DOE reduced its emphasis on security with the end of the cold war. 5. In 1999, the Secretary of Energy established a new office responsible for rebuilding security awareness and performance to ensure protection of national security. 	<ol style="list-style-type: none"> 1. In the late 1980's worker safety and health programs were considered to be secondary to both the mission and national security priorities. 2. Safety discipline was lax. Safety requirements were considered to be optional to many in the late 1980's. 3. Emphasis and priorities are different now than in the 1980s. This changed early in the 1990s because of public and Congressional pressures on DOE. 4. DOE shifted its emphasis to increase nuclear, environmental, and worker safety performance. 5. Safety has had higher priority and than security since the early 1990's.
Comparative Analysis	
<p>The priority for security awareness and safety and health has reversed. The current security awareness situation is similar to that of safety and health at the beginning of the 1990s; the priority for improving security performance across the DOE complex has been significantly altered. The public and Congress expect DOE to make significant improvements to security awareness and performance. DOE's resolve is demonstrated by the creation of the Office of Security and Emergency Operations (OSS), and by establishing an expectation that security awareness programs must improve.</p>	

Table C.3

Delivering the Awareness Message - Late 1980s to Present	
Security Awareness	Safety and Health
<ol style="list-style-type: none"> 1. In the late 1980's Security relied on subject matter experts to develop, direct implementation, and monitor security compliance. 2. External mission requirements supported security department mandates and impacts. In the 1980s individuals had to comply with security. The principle difference in awareness levels appears to be in the level of concern and priority given to Security over Safety. 3. Beginning in the 1990s, there has been reduced accountability for poor security performance, and until 1999, the DOE-wide perception was that security risks were being acceptably managed 4. Security funding was reduced in the 1990s to levels needed to maintain minimal security awareness programs 5. Health and Safety supplanted security awareness programs priorities in the 1990's. 	<ol style="list-style-type: none"> 1. Safety and Health used a similar approach 2. In the 1980s Safety and Health lacked management attention and accountability. Reduced funds and lowered management priority added to safety SMEs' sense of "pushing rope." 3. In the mid-1990s, safety approaches changed within DOE. Subject Matter Experts began getting input from the workforce on how to deploy more effectively. There is specific emphasis on getting workers and managers involved in developing safety procedures. 4. Safety received increased funding and resources in the 1990s to build safety awareness programs. 5. DOE contractors lost multi-billion dollar contracts in the 1990s because they were unsuccessful at achieving safety buy-in from the workforce using traditional approaches.

Table C.3 continued

Delivering the Awareness Message - Late 1980s to Present	
Security Awareness	Safety and Health
<p>6. Security awareness programs in the 1990's continued to make-do with the resources and processes that were in place.</p> <p>7. In the 1990's Security approach remained dependent on subject matter experts to develop, direct implementation, and monitor security compliance.</p> <p>8. Reduced funds and lowered management priority in the 1990's added to security awareness SMEs' sense of "pushing rope."</p> <p>9. Through out the 1990's Security programs maintained the processes, standard of performance and continued to assess compliance.</p> <p>10. Today, the security awareness approach has succeeded at informing employees about security requirements and has achieved compliance. However workers do not share the level of involvement or integration that has been achieved by safety programs.</p>	<p>6. DOE endorsed the Occupational Safety and Health Administration's Voluntary Protection Program in the mid-1990's.</p> <p>7. The Safety and Health approach changed. Two key principles of the Voluntary Protection Program, "Management Commitment" and "Worker Involvement," were found to be incompatible with traditional Safety and Health approaches that had been followed in the 1980s.</p> <p>8. Managers and workers were engaged by the SMEs to get their involvement in and commitment to the programs.</p> <p>9. Managers and workers wanted to have a say in the development of processes, standards of performance and evaluation of the programs.</p> <p>10. Today, the safety awareness approach has succeeded at engaging individuals, increasing their empowerment and involvement in developing safety practices that better integrate with doing work at Hanford.</p>
<i>Comparative Analysis</i>	
<p>The most significant aspect of delivering the message is that in the mid-1990s, Safety and Health took a new approach to improving performance while Security continued with the same approach it had successfully used in the 1980s. The reason Safety and Health took such a drastic approach is that despite increased funding, management involvement, and accountability at a corporate level, performance did not improve and companies lost award fees as well as their DOE contracts for failure to engage the workforce. DOE and its contractors recognized the need to find a more effective way to achieve safety performance goals. DOE implemented the Occupational Safety and Health Administration's performance based safety program called the Volunteer Protection Program (VPP). This systematic process for changing the safety culture engaged and empowered the workforce, created a safer work environment and changed the DOE safety culture. Perceptions about safety as a value improved when safety and health SME's were brought into the initial planning stages of preparing work packages. Where Safety and Health was once seen as a barrier to getting work done, it is now nearly fully integrated with the way people think about doing work and is perceived as being helpful in getting the job done right. The results of these program changes have been dramatic; Safety and Health performance at Hanford improved 65% between October 1996 and September 2000.</p>	

Table C.4

Communications Media - Late 1980s to Present

Security Awareness	Safety and Health
<p>1. Security programs used standard communications media to communicate to employees in the 1980s and early 1990s</p> <ul style="list-style-type: none"> ➤ Posters ➤ Bulletins ➤ Newsletters ➤ Articles in site newsletters ➤ Pamphlets for special issues <p>2. In many ways the security awareness approach used today is similar to that used in the late 1980s and early 1990s. However, security awareness at Hanford is augmenting the traditional approach through creative uses of the media and through new media resources.</p> <p>Security Awareness has:</p> <ul style="list-style-type: none"> ➤ Increased emphasis and interest for building a “security culture” ➤ Added security recognition and award programs (“Security Pays in Many Ways”) ➤ Created “Security Ed” Cartoon ➤ Distributed Mouse pads with security message ➤ Conducted security challenges ➤ Used emails to emphasize special topics ➤ Created the homepage security banner <p>3. Field visits by SMEs provide opportunities to share security messages effectively. They also provide opportunities to demonstrate the level of commitment to achieving a secure working environment.</p> <p>4. The awareness program has been successful at getting the workforce to comply with security but has not been as successful at instilling high levels of commitment to security principles and values.</p>	<p>1. Safety programs used standard communications media to communicate to employees in the 1980s and early 1990s</p> <ul style="list-style-type: none"> ➤ Posters ➤ Bulletins ➤ Newsletters ➤ Articles in site newsletters ➤ Pamphlets for special issues <p>2. Safety awareness programs have continued to improve the quality and variety of their communications. The attitudes, beliefs and values of VPP have permeated the communicated messages regardless of the media chosen.</p> <p>Safety and Health has:</p> <ul style="list-style-type: none"> ➤ Worker involvement in planning and conducting self-assessments ➤ Safety awards and recognition programs ➤ Tool box safety meetings ➤ Participation in safety conferences ➤ Active engagement of unions and managers in working on diverse teams to improve safety programs. ➤ Uses performance measures to motivate and communicate results <p>3. Although safety SMEs also make visits to the field, the most effective communication tool being used by VPP is employee word-of-mouth messages. These discussions include emotional content, encourage involvement and interaction, build commitment and reinforce the safety message.</p> <p>4. Safety and Health has implemented processes that engage and involve workers and managers in ways that build ownership for the principles and values of safety.</p>

Comparative Analysis

Both programs have developed more innovative ways to communicate their message, however the VPP program changes have substantially increased employee involvement in developing and communicating the safety messages. The changes have strengthened that message making it more relevant because it is the employees' message being shared with coworkers. Human interactions convey emotional messages. Relying on word-of-mouth messages is an important contributor to VPP success.

Table C.5

Message Content - Late 1980s to Present

Security Awareness	Safety and Health
<ol style="list-style-type: none"> 1. There have been improvements to some aspects of the message content. However, there is still too much reliance on cognitive messages that explain or direct rather than engage and involve the employee. 2. A "Parent to Child" message still appears occasionally in security messages and actions. This reduces the potential effectiveness of the message. The implied or direct threats that were prevalent in the early 1990's are rarely used today in Security communications. 3. The requirements and understanding of the security threats in non-Limited Area Island facilities appears to be somewhat confusing. 	<ol style="list-style-type: none"> 1. Safety is effective at engaging individuals and using descriptions of personal safety experiences submitted by employees to send more effective messages. These personal experiences often contain strong affective messages about safety. There is reliance on sharing what people feel and believe rather than on communicating the SME's message. 2. The new message from safety is based on customer service rather than enforcement. Safety communicating in VPP is based on "adult to adult" transactions. Threats are not used. Concerns for the well being of coworkers is expressed. 3. VPP places the requirement to analyze the hazards with both the employees and managers. The general approach that has been taken is to form teams to analyze and protect against the hazards in the workplace.

Comparative Analysis

In the 1980s the Security Awareness and Safety and Health programs used similar approaches in communicating to, not with, the workforce. A significant difference was that Security could better deliver on its promises of discipline because of legal backing, DOE orders, and management sponsorship for security. VPP Change safety messages to align with valuing the workforce and sharing the experiences of workers. Communicating on an adult-to-adult basis improves the interactions that bring about change.

Table C.6

Management & Worker Involvement - Late 1980s to Present	
Security Awareness	Safety and Health
<ol style="list-style-type: none"> 1. Security had strong accountability in the 1980s and early 1990's. 2. Current surveys show that workers are aware of security needs, however the interviews with Security Awareness managers throughout the DOE indicate they would like security to be perceived as a benefit rather than a "necessary evil" in getting work done. 3. The need for secrecy is in conflict with the need to engage the workforce. 	<ol style="list-style-type: none"> 1. Safety had weak accountability in the 1980s and early 1990's. 2. Involvement of managers and workers in implementing effective Safety and Health programs is a characteristic of the VPP approach. This involvement of workers and managers in developing and implementing safety processes has increased ownership and commitment to the standards that have been developed. Safety is no longer a "necessary evil," it is integrated into how work is done. 3. VPP encourages open, honest, non-punishing exchanges of information.
Comparative Analysis	
<p>The level of manager and worker involvement is a major difference between the two approaches. Safety and Health programs have achieved significant changes in attitudes, beliefs, values, behaviors and performance over the past 5 years. Security awareness programs value the individuals but do not currently engage and empower workers and managers in the development and deployment in those aspects of security that directly impact their work environment. Secrecy issues have hampered efforts to clearly communicate the risks, consequences, and frequency of security lessons learned either within the DOE or from industry experience to the general workforce. This puts the Security Awareness program at a competitive disadvantage.</p>	

Table C.7

Perceptions of Awareness Success - Late 1980s to Present	
<i>Security Awareness</i>	<i>Safety and Health</i>
<p>1. Security culture attitudes, beliefs, values and expectations have not been communicated with the clarity of the VPP program. However, interviews with Security Experts at Hanford and elsewhere in the DOE show that security experts share a consistent understanding of what a security culture looks like. Analysis of the elements discussed in these interviews identified 5 key elements of an Outstanding Security Culture. They were, in order of “frequency of identification” by managers:</p> <ul style="list-style-type: none"> ➤ Personal ownership (valuing security) ➤ Management support (commitment) ➤ Delivering the security message (effective and comprehensive) ➤ Teamwork (no more "us versus them") ➤ Performance (Proof the program is working) 	<p>1. The VPP safety culture is established by its five tenets. These concepts have been communicated consistently since 1989 within the program and since 1994 within the DOE.</p> <ul style="list-style-type: none"> ➤ Management Leadership ➤ Employee (worker) involvement ➤ Work-site analysis ➤ Hazard prevention and control ➤ Safety and health training
<p><i>Comparative Analysis</i></p> <p>Security Awareness program management attitudes are changing. There is a desire to improve communication with workers. There is interest in building ownership rather than just getting minimum compliance. Management is open to trying new approaches to achieve higher levels of awareness and security performance.</p> <p>The Security Awareness and Safety and Health programs had similar definitions for "awareness success" in the 1980s. These definitions were based on the assumption that people should do as the Subject Matter Experts directed them. The SME's held the standard and delivered it with the expectation that the workers would follow it even if they weren't committed to it.</p> <p>Security and Safety programs in the 1980s were using very similar approaches to influence the workforce. The programs used a directive approach, creating well-defined programs with clear requirements. Evaluations of compliance measured the level of performance. Security achieved compliance because the workforce understood the importance of national security, it was a clear site priority, and security personnel were empowered to enforce the requirements. Safety was much less successful in the 1980s because the management and the workforce did not value safety; it was not a site priority; and there was little accountability for lack of performance.</p> <p>Currently, there are significant similarities between the beliefs and values identified in the Security Experts' survey of what the elements of a successful security culture are, and principles described in the Volunteer Protection Program and Integrated Safety Management programs. Programs that engage and empower the workers are achieving the successful security culture described by managers.</p>	

Case Study Citations

- DOE/EH-0591, WSRC. Report from the DOE Voluntary Protection Program Onsite Review, May 1999 <http://www.inel.gov/resources/vpp/main.html>
- DOE/EH-0645, Protection Technology Hanford. Report from the DOE Voluntary Protection Program Onsite Review. August 15-18, 2000 <http://www.inel.gov/resources/vpp/main.html>
- DOE VPP Approved. Environmental Safety & Health, Safety Notes. February 1994 <http://www.inel.gov/resources/vpp/main.html>
- Habiger, Eugene E. (March 2000). Statement of Eugene E. Habiger, General, USAF (Retired), Director Office of Security and Emergency Operations, U.S. Department of Energy, Before the Senate Appropriations Committee, Energy and Water Development Subcommittee, FY 2001. Appropriations Hearings, March 28, 2000. Federation of American Scientists (FAS), Government Secrecy News
- Hanford Site Performance Report. PHMC. July 1999 <http://hanford.gov>
- McLuhan, M. (1966). The Medium is the Message. Hardwired
- Mowen, J.& Minor, M. (2001). Group, Dyadic, and Diffusion Processes. In Consumer Behavior, a Framework (p. 251). Upper Saddle River: Prentice Hall.
- PHMC Environmental Management Performance Report. PHMC. January 2001 <http://hanford.gov>
- Safety, Hanford Progress. February 2000 <http://www.inel.gov/resources/vpp/main.html>
- Safety and Health Program Management Guidelines; Issuance of Voluntary Guidelines. 54 Fed. Reg. 3904-3916. OSHA <http://www.osha.gov>
- The Principles of a Total Safety Culture. INEEL Homepage <http://www.inel.gov/resources/vpp/main.html>
- Two Hanford contractors become VPP 'Stars'. Hanford Reach. February 26, 2001
- Voluntary Protection Program (VPP) a program that's here to stay. Hanford VPP Homepage <http://hanford.gov/safety/vpp/tenets.htm>
- Voluntary Protection Program Survey Results, Calendar Year 1999. Hanford VPP Homepage <http://www.hanford.gov/safety/vpp/survey1.htm>

Appendix C



Security Pays



Security Pays



Security Pays

**IMAGINE YOU HAVE A PENCIL
STICKING OUT FROM YOUR
CHIN & SIGN YOUR FULL NAME
IN THE AIR AS LARGE AS
POSSIBLE. . .FEEL BETTER?**



Sponsored by the Security Awareness Team – Security Pays in Many Ways!

SECURITY AWARENESS SUGGESTION BOX

QUESTIONS?

IDEAS?

STORIES?

PLEASE SHARE THEM WITH US!

CLICK HERE



Sponsored by the Security Awareness Team – Security Pays in Many Ways!

Test Your Knowledge . . .



WHO WON THE 1969 WORLD SERIES?

CLICK HERE FOR THE ANSWER

Sponsored by the Security Awareness Team – Security Pays in Many Ways!

A Thought For the Day . . .

**“YOU CAN DETERMINE THE
QUALITY OF AN INDIVIDUAL BY
THE STANDARDS THEY SET
FOR THEMSELVES”**

-Anonymous



Sponsored by the Security Awareness Team – Security Pays in Many Ways!

**E-MAIL
DO'S &
DON'TS**



**CLICK HERE
FOR MORE
INFO**

Sponsored by the Security Awareness Team – Security Pays in Many Ways!

