



This is to certify that the

thesis entitled

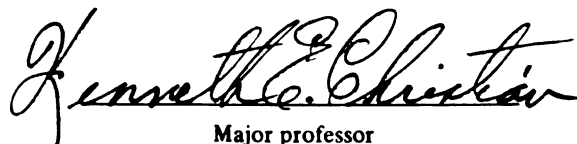
A QUALITY SECURITY COUNTERMEASURES PROCESS
FOR FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE OF
UNITED STATES DEFENSE FIRMS IN THE
NATIONAL INDUSTRIAL SECURITY PROGRAM

presented by

Daniel Joseph Muscat

has been accepted towards fulfillment
of the requirements for

Master's degree in Criminal Justice



Major professor

Date April 6, 1994



LIBRARY
Michigan State
University

PLACE IN RETURN BOX to remove this checkout from your record.
TO AVOID FINES return on or before date due.

DATE DUE	DATE DUE	DATE DUE
3/23/98		

**A QUALITY SECURITY COUNTERMEASURES PROCESS
FOR FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE OF
UNITED STATES DEFENSE FIRMS IN THE
NATIONAL INDUSTRIAL SECURITY PROGRAM**

By

Daniel Joseph Muscat

A THESIS

**Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of**

MASTER OF SCIENCE

School of Criminal Justice

1994

rep

reg

cla

(TQ

effe

inhe

of d

W. Ec

impro

flaws

NISP

PDSA e

profes

77 res

as pra

conside

ABSTRACT

A QUALITY SECURITY COUNTERMEASURES PROCESS FOR FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE OF UNITED STATES DEFENSE FIRMS IN THE NATIONAL INDUSTRIAL SECURITY PROGRAM

By

Daniel Joseph Muscat

The National Industrial Security Program (NISP) replaces conflicting Executive Branch industrial security regulations with an integrated strategy to safeguard U.S. classified information. Resource Total Quality Management (TQM) drives this effort to develop an efficient, cost-effective security posture.

One complex NISP issue is technology transfer risk inherent in foreign ownership, control, or influence (FOCI) of defense firms. This research focuses on whether TQM guru W. Edwards Deming's "Plan, Do, Study, Act" (PDSA) process improvement theoretical model will aid efforts to detect flaws in current countermeasures and help define an enhanced NISP process. Process improvement ideas resulting from the PDSA exercise are rated by an opinion survey of 114 security professionals from FOCI and non-FOCI firms. The majority of 77 respondents (36% FOCI, 64% non-FOCI) rate 10 of 12 ideas as practical process improvements, suggesting they merit consideration in the National Industrial Security Program.

Copyright by
Daniel Joseph Muscat
1994

DEDICATION

To my wife Carole,
and my daughters, Melissa and Kristi,
in appreciation of all your love, and support.

ACKNOWLEDGMENTS

The author would like to acknowledge the assistance, dedication, and professionalism of the faculty and staff of the Leadership and Management Program in Security in the School of Criminal Justice at Michigan State University. Individuals who deserve special recognition include thesis chair, Dr. Kenneth E. Christian, Dr. Frank S. Horvath, Dr. David L. Carter, and Dr. Merry Morash. Finally, special thanks are extended to Assistant Deputy Undersecretary of Defense for Security Policy, Mr. Maynard C. Anderson, a recognized leader in the security community, who generously shared his wisdom during this research.

List

List

I.

II. I

A

B

C.

D.

E.

F. C

A

TABLE OF CONTENTS

	<u>Page</u>
List of Figures.	ix
List of Abbreviations.	xi
I. Introduction.	1
A. Total Quality Management: A U.S. National Secret that became the Secret to Safeguarding U.S. National Secrets	1
B. National Industrial Security Program and TQM .	5
C. Foreign Ownership, Control, or Influence: A Complex Security Issue	10
II. Literature Review	18
A. Deming's Cycle: An Operational Definition of the Plan, Do, Study, Act (PDSA) Theoretical Model.	18
B. Defining Foreign Ownership, Control, or Influence	23
C. Defining U.S. Foreign Investment Policy. . . .	25
D. Defining U.S. Foreign Investment Regulations.	27
E. Defining the Evolution of Defense Industrial Security Program Foreign Ownership, Control, or Influence Security Regulations.	30
Board Resolutions.	39
Reciprocal Facility Clearances	40
Voting Trust Agreements.	41
Proxy Agreements	42
Special Security Agreements.	42
F. Globalization Future Shock: Thomson CSF Attempts to Acquire LTV.	44

III. Methodology - Deming's Cycle: Plan, Do, Study, Act	48
A. "Plan" Step One: Identification of the Opportunity for Improvement.	48
B. "Plan" Step Two: Documenting the Present Process in a Critical Examination of FOCI Security Regulations	54
<u>Positive Notes - What Works</u>	
1. Consistency with Foreign Investment Policy.	57
2. Defense Technology Access	59
3. Defense Security Committee.	61
4. Security Awareness.	67
5. Export Control Compliance	68
<u>Negative Notes - What Needs Work</u>	
6. FOCI National Security Intelligence, Threat Assessment and Risk Analysis	70
a. Collection	72
b. Evaluation of Reliability and Validity .	74
c. Integration and Analysis	76
d. Dissemination.	79
7. National Interest Determination	81
8. Proscribed Information.	87
9. Threat Emphasis and Security Countermeasure Development.	92
10. Security Agreement Violation Clauses. . . .	96
11. Personnel Security.	100
12. Security Awareness, Training and Education.	101
C. "Plan" Step Three: Envisioning an Improved NISP FOCI Security Countermeasures Process. . .	107

Footno

Biblio

D. "Plan" Step Four: Scoping the NISP FOCI Security Countermeasures Process Improvement Plan.	110
1. Management Plan	110
2. NISP FOCI Security Policy Proposal.	120
E. "Do" Step Five: Survey of Security Professionals	158
1. Survey Objectives.	158
2. Survey Instrument and Responses.	160
F. "Study" Step Six: Studying the Survey Results.	194
G. "Act" Steps Seven and Eight: Conclusions, Actions Required for the NISP, and Recycling PDSA.	199
Footnotes	200
Bibliography.	201

- 1.1 Natio
Task
- 1.2 The D
- 2.1 Defin.
- 2.2 The T
- 2.3 Depart
DD For
- 2.4 Depart
Pertai
- 3.1 The Vo
curren
(An ad
- 3.2 DISP F
- 3.3 NISP F
- 3.4 FOCI A
- 3.5 FOCI A
- 3.6 Concep
Threat
- 3.7 Securi
Voting
- 3.8 Securi
Proxy
- 3.9 Securi
Recipr
- 3.10 Securi
Board

LIST OF FIGURES

	<u>Page</u>
1.1 National Industrial Security Program Task Force 22 January 1991	8
1.2 The Deming PDSA Cycle (Scherkenbach, 1991, p.61) .	15
2.1 Definition of a Process (Scherkenbach, 1991, p.8).	20
2.2 The Two Voices (Scherkenbach, 1991, p. 11)	21
2.3 Department of Defense Security Agreement DD Form 441.	32
2.4 Department of Defense Certificate Pertaining to Foreign Interests DD Form 441S . . .	35
3.1 The Voice of the Customer (NISP) versus the two current Voices of the Process (SSA or Trust/Proxy) (An adaptation of Scherkenbach, 1991, p. 78) . . .	50
3.2 DISP FOCI Adjudication Process Model	55
3.3 NISP FOCI Adjudication Process Model	109
3.4 FOCI Adjudication Guidelines, Part 1	114
3.5 FOCI Adjudication Guidelines, Part 2	115
3.6 Conceptual Example of a FOCI Threat Assessment Matrix	116
3.7 Security Professional Ratings Voting Trust Agreement Effectiveness	165
3.8 Security Professional Ratings Proxy Agreement Effectiveness.	166
3.9 Security Professional Ratings Reciprocal Clearance Effectiveness	167
3.10 Security Professional Ratings Board Resolution Effectiveness	168

3.11 Security
Spec

3.12 Rating
General
Police

3.13 Rating
National

3.14 Rating
Threat

3.15 Rating
Part

3.16 Rating
Adjud

3.17 Rating
with
Voting

3.18 Rating
Security

3.19 Rating
Access

3.20 Rating
Training
Direct

3.21 Rating
Training
Security

3.22 Rating
Training
Agency

3.23 Rating
Training
Overs

3.11	Security Professional Ratings Special Security Agreement Effectiveness	169
3.12	Ratings of the National Disclosure Policy/ General Security of Information Agreements FOCI Policy Foundation Idea	174
3.13	Ratings of the New, Three Step, National Interest Determination Process Idea	176
3.14	Ratings of the FOCI Threat Assessment Committee Idea	178
3.15	Ratings of the Automated Form 441S "Certificate Pertaining to Foreign Interests" Idea.	180
3.16	Ratings of the NISP FOCI Adjudication Committee Idea.	182
3.17	Ratings of the NISP 441 Security Agreement with FOCI Amendments versus Voting Trust/Proxy/SSA Idea.	184
3.18	Ratings of the Proscribed Data Security Countermeasures Idea.	186
3.19	Ratings of the Security Assurance, SF 312, Limited Access Authorization for Foreign Directors Idea.	188
3.20	Ratings of the Security Awareness, Training and Education for Outside Directors/Proxies/Trustees Idea.	190
3.21	Ratings of the FOCI Security Awareness, Training and Education for Facility Security Officers Idea	191
3.22	Ratings of the FOCI Security Awareness, Training and Education for Procurement Agency Officials Idea.	192
3.23	Ratings of the FOCI Security Awareness, Training and Education for NISP Oversight Agency Officials Idea.	193

AIA

CFIUS

CIA

COMSEC

CSO

DASD CI/

DASD C³I

DD Form 4

DD Form 4

DDL

DIA

DIS

DISCO

DISP

DoD

DoE

DSC

ECO

ESC

FBI

LIST OF ABBREVIATIONS

AIA	Aerospace Industries Association
CFIUS	Committee on Foreign Investment in the U.S.
CIA	Central Intelligence Agency
COMSEC	Communications Security
CSO	Cognizant Security Office
DASD CI/SCM	Deputy Assistant Secretary of Defense, Counterintelligence/Security Countermeasures
DASD C³I	Deputy Assistant Secretary of Defense, Command, Control, Communications, and Intelligence
DD Form 441	Defense Department Form 441 Security Agreement
DD Form 441S	Defense Department Form 441S Certificate Pertaining to Foreign Interests
DDL	Decision Disclosure Letter
DIA	Defense Intelligence Agency
DIS	Defense Investigative Service
DISCO	Defense Industrial Security Clearance Office
DISP	Defense Industrial Security Program
DoD	Department of Defense
DoE	Department of Energy
DSC	Defense Security Committee
ECO	Export Control Officer
ESC	Executive Security Committee
FBI	Federal Bureau of Investigation

FCL

FOCI

FOCI/AC

FOCI/TAC

FSO

GAO

GSOIA

HOF

ISOO

ISM

LAA

MFO

NATO

NDP

NID

NISP

PCL

PDSA

PMF

SATE

SF 312

SSA

TCP

TQM

FCL	Facility Clearance
FOCI	Foreign Ownership, Control, or Influence
FOCI/AC	FOCI Adjudication Committee
FOCI/TAC	FOCI Threat Assessment Committee
FSO	Facility Security Officer
GAO	General Accounting Office
GSOIA	General Security of Information Agreements
HOF	Home Office Facility
ISOO	Information Security Oversight Office
ISM	Industrial Security Manual for Safeguarding Classified Information (DoD 5220.22-M)
LAA	Limited Access Authorization
MFO	Multiple Facility Organization
NATO	North American Treaty Organization
NDP	National Disclosure Policy
NID	National Interest Determination
NISP	National Industrial Security Program
PCL	Personnel Security Clearance
PDSA	Plan, Do, Study, Act
PMF	Primary Management Facility
SATE	Security Awareness, Training and Education
SF 312	Standard Form 312 - Classified Information Nondisclosure Agreement
SSA	Special Security Agreement
TCP	Technology Control Plan
TQM	Total Quality Management

A. Total
Became

The

War Depa

for mate

its indu

the Depa

largely b

colleague

earlier,

he publis

ations in

that monit

informatio

its future

ing the hu

to fight t

of the war

quality tec

an irony of

fifty years

to a highly

I. INTRODUCTION

A. Total Quality Management: A U.S. National Secret that Became the Secret to Safeguarding U.S. National Secrets

The year was 1942, and as World War II raged, the U.S. War Department (Pines, 1990) faced an unprecedented demand for materials to aid the Allied cause. Turning to one of its industry suppliers Bell Telephone Laboratories for help, the Department established a Quality Control section staffed largely by Bell employees who employed the ideas of their colleague, statistician Walter A. Shewhart. Eleven years earlier, Shewhart succeeded in making quality a science when he published his thoughts on "statistical control" of variations in manufacturing processes. Shewhart's work proved that monitoring manufacturing according to measurable information could bring a process under control and make its future predictable. Statistical control of manufacturing the huge quantities of ships, tanks, and planes needed to fight the Axis power quickly became a critical element of the war effort. In fact, at one point Shewhart's quality techniques became classified military secrets. In an irony of history that would not play out for almost fifty years, national defense requirements had given birth to a highly guarded, valuable "body of quality knowledge."

follow

nation

Shewha

suppli

quality

unsucce

broader

and an

the awkw

to an in

quality.

the press

the U.S.

battle.

were each

economy.

their surv

with their

control ov

hearkened

after loosi

global econ

Scores

management

Walton; and

Deming's no

Ellis Pines (1990) highlighted that one of Shewhart's followers, W. Edwards Deming, later to become one of the nation's foremost quality gurus, taught many courses on Shewhart's quality methods to numerous defense industry suppliers during the war. When the conflict ended the quality techniques were declassified and Deming tried unsuccessfully to sell his quality education courses to a broader spectrum of U.S. businesses. Post war prosperity and an insatiable demand for consumer goods put Deming in the awkward position of trying to preach his quality message to an industrial audience more concerned with quantity than quality. Thus, in July 1950, Deming went to Japan and told the presidents of that country's leading manufacturers about the U.S. military secret that had helped defeat them in battle. These leaders, representing diverse industries, were each striving to re-establish a still faltering economy. Deming told them that quality was essential to their survival, and he urged them to work in partnership with their vendors, to develop instrumentation and to gain control over their processes. Japanese top management hearkened Deming's words on quality, and some thirty years after loosing the military battle, they began to win the global economic war.

Scores of books have been written on Deming's theory of management (Aguayo; Deming; Nadler et.al; Scherkenbach; Walton; and many more). Most cite, then further develop, Deming's now famous "fourteen points" which he described as

princi

1986 b

fourte

transfo

(PDSA)

PDSA is

the Plan

the scie

after Wa

quality

William S

Continual

ways to c

(1991) ad

in fact, r

tasks or p

solved, bu

does, of c

In the

recession,

search of e

had incurre

(Pines, 199

imports too

toured Japa

long to dis

Deming star

principles for transformation of western management in his 1986 book Out of Crisis. In describing point number fourteen, "Take action to accomplish the (quality) transformation," emphasis is placed on the Plan-Do-Study-Act (PDSA) circular model Deming introduced to the Japanese. PDSA is Deming's improvement on what many observers know as the Plan-Do-Check-Act (PDCA) model. Frequently compared to the scientific method, Deming called it the Shewhart Cycle after Walter Shewhart, the Bell Labs pioneer of statistical quality control. The Japanese called it the Deming Cycle. William Scherkenbach's book (1991) Deming's Road to Continual Improvement focuses heavily on PDSA and explains ways to convert the theory into practice. Mary Walton (1991) adds perspective by suggesting that the Deming Cycle, in fact, represents work on processes rather than specific tasks or problems. Processes by their nature can never be solved, but only improved. In working on processes, one does, of course, solve some problems.

In the late 1970s and early 1980s, mired in a deep recession, American executives journeyed to the Pacific in search of explanations for the huge market share losses they had incurred to Japanese imports. Ford Motor Company alone (Pines, 1990) lost \$1.6 billion in 1980 when automobile imports took 26.7 percent of the U.S. market. As they toured Japanese factories, it did not take U.S. executives long to discover that the commitment to quality inspired by Deming started at the top of the corporate ladder and flowed

all

Japa

Give

Total

topic

Numer

more v

qualit

involv

where "

reverse

the big

TQM

Defense

General

was appo

Having ac

quality u

issued a

"We will i

coordinated

Strategy."

Defense, Fr

efforts the

the Departm

all the way to the factory floor. Pines points out that the Japanese effort toward quality was, in a word, "total."

Given the American passion for buzzwords, the concept of Total Quality Management, or TQM, quickly became the hottest topic in business schools, books, and professional seminars. Numerous consulting firms popped up, each focusing on one or more variations of the same process improvement theme: quality function deployment; just in time; employee involvement; design of experiment, to name a few. Ford, where "Quality" became "Job 1," adopted Deming's methods, reversed its downward spiral, and went on to become one of the biggest TQM success stories.

TQM found its way back to the U.S. military, by now the Defense rather than War Department, in 1987 when former General Motors executive and Deming disciple Robert Costello was appointed Undersecretary of Defense for Acquisition. Having achieved remarkable improvements in automotive quality using Deming tools, on October 5, 1987 Costello issued a memo to the military departments that announced, "We will integrate all our efforts related to quality into a coordinated Department of Defense Total Quality Management Strategy." In March 1988, newly appointed Secretary of Defense, Frank Carlucci gave Costello's quality improvement efforts the needed top management commitment making TQM in the Department of Defense (DoD) official.

B. National Industrial Security Program and TQM

By coincidence, in March 1988, security professionals in the Aerospace Industries Association (AIA) unknowingly jumped on Costello's DoD TQM bandwagon when they conceptualized the National Industrial Security Program (NISP). The NISP focuses on the methods and processes employed by the government and industry to safeguard classified information in industry. An initiative to replace a plethora of overlapping, often conflicting government regulations with a single, coherent and integrated security strategy, the NISP was endorsed by President George Bush. The NISP has evolved into a government-industry response to the challenge for a more efficient and cost-effective method to ensure national security. In an era of diminishing resources, the NISP will standardize security policies and procedures throughout the Executive Branch and make available hundreds of millions of federal and private sector dollars for redirection. Herein lies the irony of history. Process improvement through TQM, a national secret during World War II, emerged years later as the secret to improving the process of safeguarding U.S. national secrets. However, as Pines suggests, the TQM story continues.

In late 1988, after further defining the concept, AIA security professionals introduced the NISP to select government security executives. Interest in the concept increased when AIA provided cost data (Atwood, Watkins,

Webst

tion

during

repres

104,00

approx.

securit

million

governm

security

these la

potentia

fifteen t

observers

examples

overly bur

In 19

chief exec

companies,

Committee.

support for

that the Ja

Carlucci cl

instrumenta

merits of a

briefings.

cost saving

Webster, 1990) for industrial security program implementation in a sample of fourteen major aerospace companies during calendar year 1989. The fourteen companies represented one-thousand cleared facilities employing 104,000 security cleared employees. These firms spent approximately \$800 million in calendar year 1989 on security. It was also estimated that approximately \$120 million could have been saved by these companies if the government were to adopt a single standard for personnel security background investigations. While the data from these large firms provided a skewed picture, the full potential for cost savings extrapolated over more than fifteen thousand defense contractors caused many skeptical observers to sit up and take notice. There were many other examples of industrial security practices that had become overly burdensome and costly following World War II.

In 1989 support for the NISP concept was received from chief executive officers of more than twenty major aerospace companies, many of whom sit on the influential AIA Executive Committee. Once again the criticality of top management support for a TQM effort was demonstrated, an imperative that the Japanese, Ford Motor Company, and Defense Secretary Carlucci clearly understood. The AIA chief executives were instrumental in facilitating opportunities to tout the merits of a NISP in Executive Branch cabinet-level briefings. The common sense premise and the potential for cost savings inherent in the concept evoked an

overw

heads

Presid

R

April

docume

in-dep

the Wh

and the

1990) s

The

eco

men

dif

We

by

int

pro

tech

In accept

In c

vari

we m

effe

tech

The Presid

industry i

status rep

Accord

and organiz

Task Force

Center, For

overwhelmingly positive response from many government agency heads, including the National Security Advisor to the President.

Responding to the government and industry support, in April 1990, President Bush signed a National Security Review document tasking the Secretary of Defense to coordinate an in-depth interagency NISP feasibility study. The report to the White House by the Secretaries of Defense and Energy, and the Director of Central Intelligence (Atwood et al., 1990) stated:

The globalization of industry, coupled with increased economic competition and dramatic strategic developments in East-West relations, will lead to new and different threats from both old and new adversaries. We agree that now is the time for a collective effort by government and industry to establish the single, integrated and cohesive security program needed to protect our economic interests and preserve our technology position of leadership.

In accepting the report, President Bush (1990) responded:

In our efforts to anticipate the scope and pace of various intelligence threats in a changing environment, we must ensure that our industrial security programs effectively and efficiently protect our vital technologies and sensitive information.

The President indicated he was pleased with plans to include industry in development of the concept and requested a status report by September 1991.

Accordingly, on 22 January 1991, the initial planning and organization meeting of the NISP Government-Industry Task Force (Figure 1.1) convened at the Interagency Training Center, Fort Washington, Maryland. The Task Force

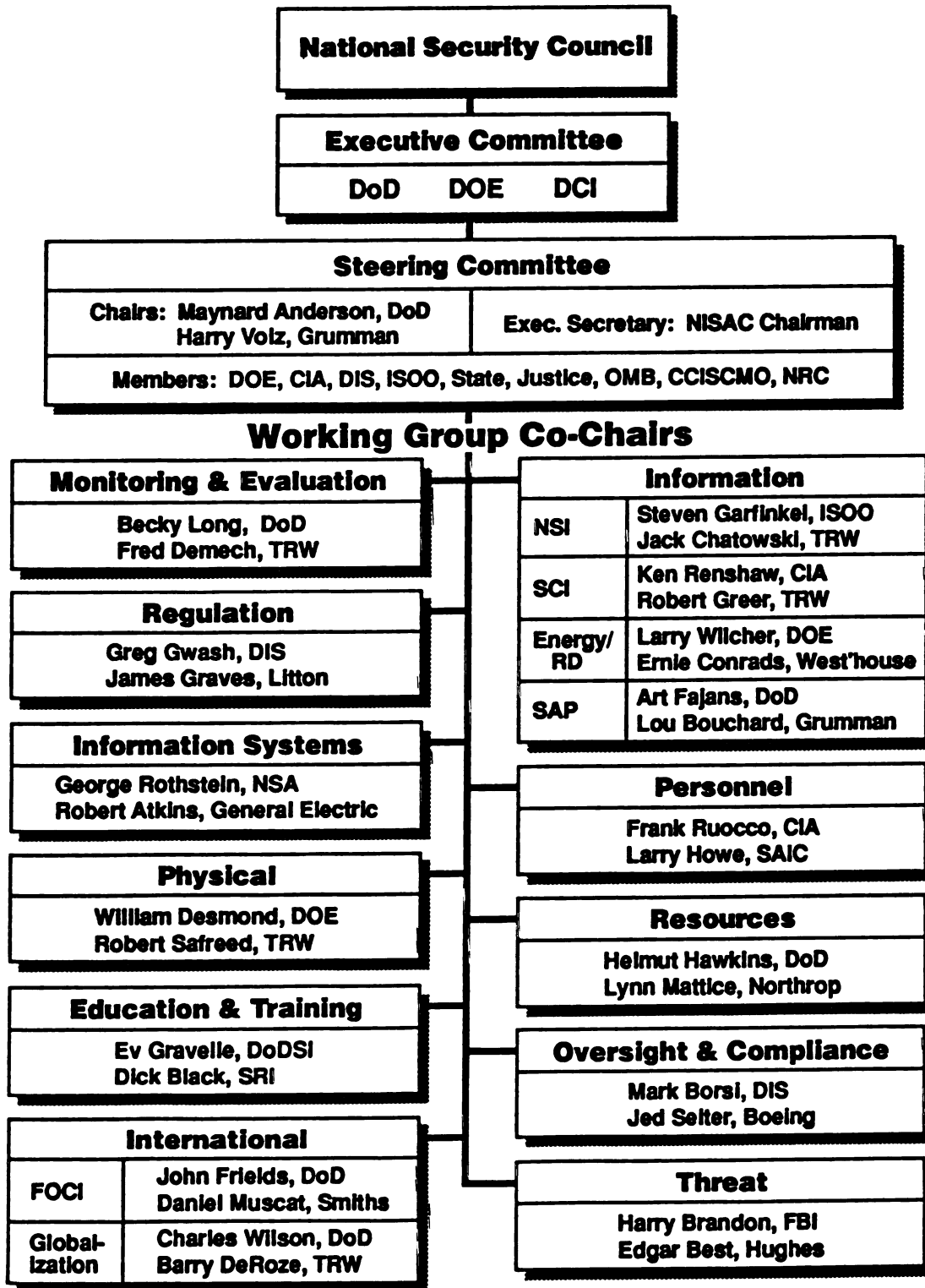


Figure 1.1

National Industrial Security Program Task Force
22 January 1991

S

a

a

s

N

pu

pl

re

we

Thu

TQM

zea

ini

hun

occ

imp

Tas

199

Ind

pro

pro

Steering Committee formed Working Groups, with government and industry representatives appointed as co-chairs, to address the various security disciplines of consequence to successful NISP implementation. During the ensuing weeks, NISP Working Group charters and objectives were published pursuant to Steering Committee procedural controls and planning milestones. Executive Branch department and agency representatives, and select industry security professionals were recruited by the co-chairs of each Working Group. Thus, the NISP transitioned from an innovative idea to apply TQM to industrial security, which was supported by a few zealous security professionals, into a Presidential initiative involving numerous government agencies and hundreds of people. Institutionalization of the NISP occurred when President Bush (1993, January 6) signed the implementing Executive Order 12829. In accordance with a Task Force commitment made to the President in a September 1991 (Atwood, Watkins, Kerr) NISP Report, a National Industrial Security Program Operating Manual would promulgate the new standardized security policies and procedures one year from that date.

I
R
C
S
th
co
De
hi
cha
ly
to
tra
vent
the

"cold
will
Commu
Zone,
U.S. E
Regula
exchange
priorit

C. Foreign Ownership, Control, or Influence:
A Complex Security Issue

A myriad of social, political, and economic changes in the world has caused government and industry security professionals to reevaluate the effectiveness of traditional methods used to safeguard valuable national security and corporate assets. In particular, the collapse of the former Soviet Union has prompted a need to redefine the sources of threat in order to implement the necessary national security countermeasures. The Assistant Deputy Under Secretary of Defense for Security Policy, Maynard Anderson (1992) highlighted the enormity of this task when he suggested the changing world economic and political picture is particularly challenging because industrial security policy is forced to change rapidly in order to keep up with new international trade agreements, treaties, the unique aspects of joint ventures among both nations and companies and, in general, the globalization of the defense market.

Indeed it seems the military confrontations of the "cold war" era are being replaced by an economic war that will be played on the battle fields of the European Economic Community, the Pacific Rim, the North American Free Trade Zone, and other market alliances that are sure to develop. U.S. Export Administration and International Traffic in Arms Regulations are being revised to accommodate more free exchange of technical knowledge. National security priorities to prevent the loss of technology to foreign

na

ir

sa

su

ha:

con

the

all

into

as t

the

Soci

iron

busi

envi

the

corp

expo

comm

thre

redra

prese

exace

firms

compl

nations bent on military superiority have become indistinguishable from corporate security priorities to safeguard proprietary information essential to business survival. The cloak and dagger image of military espionage has spawned the progeny of blatant industrial espionage for competitive advantage as the world moves closer to realizing the concept of the "stateless" corporation whose only allegiance is to its stockholders. Unemployed military intelligence officers are finding new career opportunities as they apply their trade to the market research needs of the private sector. These specialists have even created the Society of Competitive Intelligence Professionals that, ironically, espouses ethical standards in conducting the business of industrial espionage.

The foregoing provides a glimpse of the dynamic threat environment security executives involved in the design of the NISP face as they endeavor to protect government and corporate sensitive material, automated information systems, export-controlled or defense-critical technologies, and commercial secrets. Clearly, the sophistication of security threats is increasing as rapidly as world maps are being redrawn. Downsizing in government and industry, and ever-present requirements to do more with less, only further exacerbate the problem.

Foreign Ownership, Control or Influence (FOCI) of U.S. firms doing classified government work is one of the more complex security challenges facing the NISP architects as

S
t
i
C
pe
ma
re
fi
ma
str
a b

all
that
trad
naga
inte
the g
almos
alone
various

evidenced by the creation of a working group specifically focused on that subject. Inherent in the trend toward market globalization is an intensified interest in the national security implications of foreign direct investment in companies supporting the national defense, along with other more obscure forms of control, or influence. The Wall Street Journal's Rick Wartzman (1992, November 2) reports that during the 1980s some \$300 billion of foreign direct investment poured into the United States, and according to Commerce Department figures, foreigners control about 5 percent of the economy and 14.7 percent of the nation's manufacturing assets. As defense budgets shrink and the recession continues, an increasing number of U.S. defense firms are selling off parts or all of their operations. In many cases, assets are sold to foreign investors who bring strong foreign currencies or lots of cheap dollars to pursue a beachhead in the U.S. marketplace.

Additionally, companies, even countries are looking for alliances, joint venture partners and new markets in places that were previously forbidden by national or international trade embargoes. Stratford Sherman asserts in Fortune magazine (1992, September 21) that alliances have become an integral part of contemporary strategic thinking. Now that the global marketplace has reached adolescence, it seems almost everyone is under the covers with everyone else. IBM alone has joined in over 400 strategic alliances with various companies in the U.S. and abroad. Sherman also

l

i

c

tl

tr

in

co

ha

wo

Rep

com

nee

res

spa

for

fin

U.S

bud

att

amo

sec

est

nece

tow

reports that the rate of joint venture formation between U.S. companies and international partners has been growing by 27 percent annually since 1985.

The possibility that key segments of defense-related industries could come under foreign control is one of the central concerns in the debate about increased investment in the United States (GAO, 1990). In Congress, and in parts of the Executive Branch, there are hawks and doves on foreign investment. The hawks cite national security to back their cold war protectionist viewpoints. The doves, on the other hand, encourage foreign investment to reduce U.S. economic woes. In a non-partisan Congressional Research Service Report, Gary Pagliano (1992) suggests that in addressing the complex issues of foreign investment, U.S. policymakers will need to exercise caution. The application of too many restrictions could be detrimental to the country, by sparking retaliation against U.S. overseas investment and by forcing the U.S. Government, in some cases, to provide financial support to ailing companies. It could disrupt U.S. alliance relations at a time when declining defense budgets make cost-sharing among countries increasingly attractive. It could also disrupt cost-sharing agreements among U.S. and foreign companies in non-defense and dual-use sectors. A major challenge for policymakers will be to establish the appropriate balance between prudent or necessary regulation, and facilitation of the momentum toward increasing international economic cooperation.

i
t
co
is
qua
dev
effe

surre
the F
Manag
by Wal
Specif
the de
securit
countern
with Dem
model (Fi
the PDSA
current FC
importantl

Crafters of FOCI security policy in the NISP must be cognizant of, and consistent with, prevailing national foreign direct investment policy. At the same time, they can ill afford to get caught up in the complex and often emotional political debate over the benefits and detriments of increased foreign direct investment in the U.S. defense industrial base¹. To successfully complete their mission they must overlook the politics and deal with FOCI as a complex, yet increasingly important security management issue. Only then will they be able to determine whether a quality, threat driven FOCI security strategy can be developed that embraces the NISP goals of efficiency, cost-effectiveness, and Executive Branch standardization.

This study capitalizes on the historical irony surrounding development of TQM and the NISP by approaching the FOCI security question utilizing Total Quality Management continuous process improvement theory developed by Walter Shewhart and popularized by W. Edwards Deming. Specifically, foreign ownership, control, or influence of the defense industry in the NISP is reviewed, not as a security policy, but rather in the context of a security countermeasures process. Analysis is organized in accord with Deming's Cycle, the "Plan, Do, Study, Act" theoretical model (Figure 1.2). The research focuses on whether use of the PDSA methodology will aid efforts to detect flaws in the current FOCI security countermeasures process, and more importantly, assist in the identification of a strategy for

pr
ob
sta
pro
oth
asse
succ
Sche
sugge
in no
in the
measur

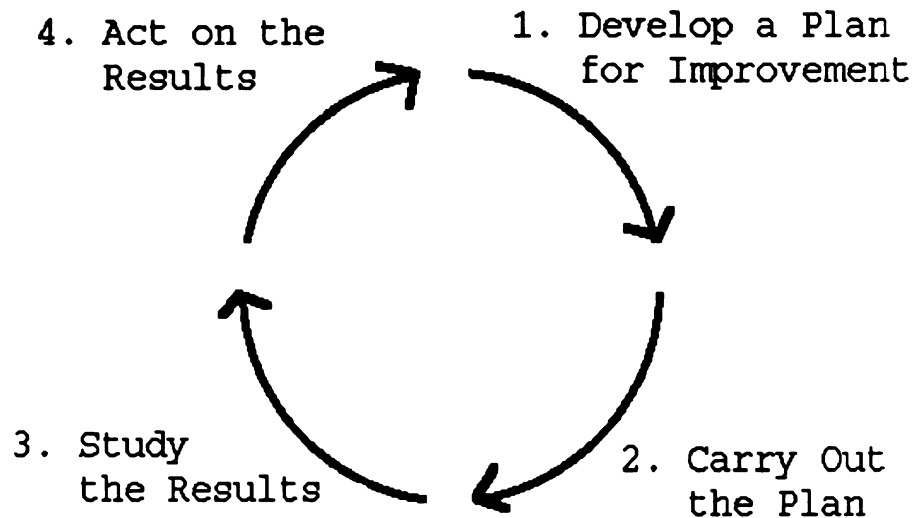


Figure 1.2

The Deming PDSA Cycle (Scherkenbach, 1991, p. 61)

process improvement that incorporates the NISP quality objectives. While Shewhart and Deming focused on statistical measures of variation in manufacturing processes, the effective application of TQM in numerous other management challenges provides a basis for the assertion that some of its precepts can be applied successfully to the FOCI national security issue. Scherkenbach (1991) lends support to this idea when he suggests that most of the opportunities for improvement are in non-manufacturing processes, for 86 percent of the people in the U.S. are engaged in non-manufacturing endeavors. The measure of success, or quality improvement, resulting from

this
signa
profe
appli
secur

it is
concep
types
foreign
control
(DISP)

the evo
present
descript
acquire
introduc
while si
continuou

Buil
defining
is then in
phase of t
the opport
process is
strengths a
of an effid

this particular PDSA exercise lies in the statistical significance of a sample of opinions by industry security professionals which either affirm or dispute the idea that application of the Deming Cycle provides an enhanced FOCI security countermeasures process model.

To establish a foundation for addressing this problem, it is first necessary to operationally define a number of concepts including: the Deming Cycle of PDSA; the various types of foreign direct investment in the U.S.; current U.S. foreign investment policy; its associated regulatory controls; and finally, Defense Industrial Security Program (DISP) FOCI security regulations. The forces influencing the evolution of the industrial security regulations are presented as a chronology culminating with a brief description of the controversial Thomson CSF attempt to acquire LTV. This overview provides the necessary introduction to the complexities of the subject matter, while simultaneously demonstrating the need to apply the TQM continuous process improvement PDSA methodology.

Building on the operational framework established by defining the relevant FOCI terminology, the PDSA methodology is then invoked. There are several steps in the "Plan" phase of the Deming Cycle, starting with identification of the opportunity for process improvement. The present process is then documented in a critical review of its strengths and weaknesses. Next, focusing on the feasibility of an efficient, cost-effective NISP Executive Branch FOCI

secu

impr

qual

is d

prof

facto

devel

avoid

secur

and f

arran

resul

drawn

adjus

ment

the g

admin

to ac

this

more

class

forei

security policy standard, the scope of a vision for an improved process is presented and rationalized.

In the "Do" phase of the Deming Cycle, where the quality improvement ideas are tested, a survey questionnaire is developed to gather opinion data from industry security professionals on the merits of process improvement ideas factored into a draft NISP FOCI Security Policy proposal developed during the "Plan" phase of the Deming Cycle. To avoid bias, surveys are administered to a sample of 114 security professionals representing both U.S.-owned firms and firms operating under current DoD FOCI security arrangements.

Then, in the "Study" phase of the Deming Cycle, survey results are observed, findings quantified, and conclusions drawn. The last phase of the Deming Cycle, "Act," where adjustments are made to take advantage of process improvement opportunities, is addressed as a summary. It is up to the government policymakers responsible for promulgation and administration of FOCI policy and security countermeasures to act, or choose not to act, upon the findings presented in this paper. Regardless of the outcome, as Deming suggests, more will be known about the process of safeguarding classified and sensitive national security information in foreign owned, controlled, or influenced firms in the NISP.

f
h
h
d
C
l
t
b
c
s
i
s
y
o
ur
na
sc
wh

co
fa
met
wit

II. LITERATURE REVIEW

A. Deming's Cycle: An Operational Definition of the Plan, Do, Study, Act (PDSA) Theoretical Model

One of the most powerful ideas that Deming presented in his lectures on quality control in Japan (Aguayo, 1990), beginning in 1950, was the Cycle of Continual Improvement based on ideas first expounded by Shewhart. Walton (1986) demonstrates Deming's feelings about the importance of the Cycle by highlighting a quote from Deming himself during a 1985 seminar. He said, use of the Shewhart Cycle will lead to continual improvement of methods and procedures. It can be applied to any process and can be used to find special causes detected by statistical signals. Walton goes on to suggest that every activity is a process and can be improved. Aguayo (1990) lends support to these arguments by suggesting that as you improve your process, you improve your knowledge of the process at the same time. Improvement of the product and process goes hand in hand with greater understanding and better theory. Aguayo points out that maybe this is nothing more than the application of the scientific method to business, but it is the only place where he had seen it done.

Scherkenbach (1987) describes the Deming Cycle of continual improvement, or Plan, Do, Study, Act (PDSA), in a fashion consistent with Aguayo's analogy to the scientific method. Scherkenbach suggests that the theory could start with a hunch or it could be as certain as a law of nature or

o
a

d
ex
in
He
se
res
ter

we
tion
thou
Cust
in p
peopl
Custo
source

physics. The result should not only be the statement of the theory but also the plan by which the theory is tested. The only purpose of collecting data or conducting an experiment or test is to form the basis of rational prediction.

According to Scherkenbach, Dr. Deming said that anyone may predict anything that he wishes but he (Deming) is only interested in rational predictions. That is to say, those predictions that have roots based in theory. It is important to make your predictions before the experiment is conducted because too many people can "prove" anything afterward.

Scherkenbach (1991) provides an excellent operational definition of the Deming Cycle for process improvement by explaining it in terms of eight action steps for implementing the four phases of the Plan-Do-Study-Act methodology. He cautions that some trips through the Cycle result in setbacks; other trips result in no apparent change; others result in improvement. But first, Scherkenbach defines the term "process" as virtually everything we do and everything we think. In its simplest form, a process is a transformation of inputs into outputs (Figure 2.1) which are often thought of in terms of customer and supplier relationships. Customers and suppliers do not have to be people. Resources in processes, that are both inputs and outputs, include: people; method; material; equipment; and environment. Customer and supplier transactions are facilitated by two sources of communication: the Voice of the Customer and the

Vo

in

to

St

Cus

Cyc

the

com

pre

high

Voic

docu

diag

ident

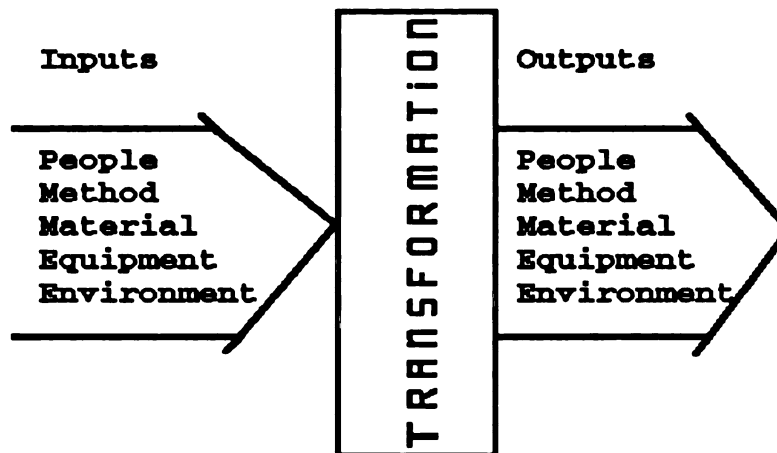


Figure 2.1

Definition of a Process (Scherkenbach, 1991, p. 8)

Voice of the Process. The objective of the PDSA process improvement methodology is therefore, to continuously strive to eliminate variance in this communication (Figure 2.2). Stated simply, the goal is to align the Voice of the Customer with the Voice of the Process.

According to Scherkenbach, the "Plan" phase of the PDSA Cycle has four steps. Step one is to recognize and identify the opportunity for process improvement. This involves comparison of the present Voice of the Customer with the present Voice of the Process. This action will highlight the variance or gap between the two process Voices. Then, in step two, the present process is documented, preferably in the form of a process flow diagram. Step three operationally defines the opportunity identified in step one by creating a vision of the improved



process

is deve

incorpor

as the s

The

the pilo

is carri

the custo

organizat

resources

environmen

In th

action plan

The purpose

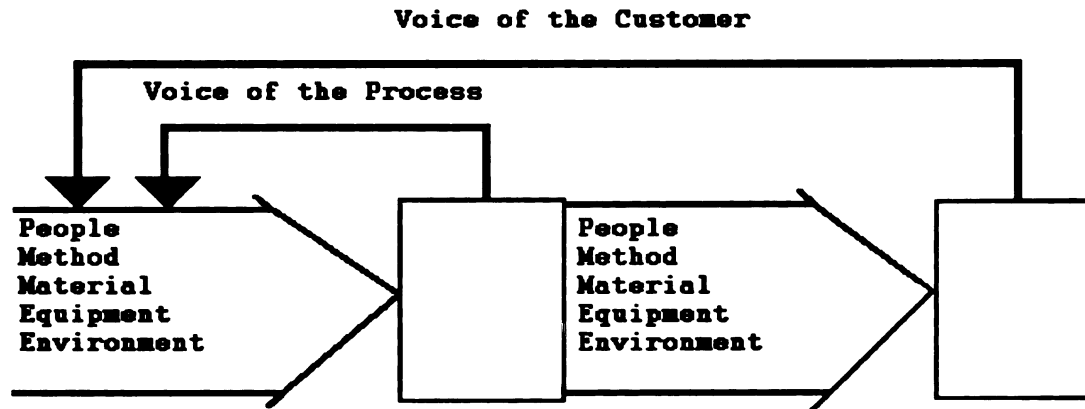


Figure 2.2

The Two Voices (Scherkenbach, 1991, p. 11)

process. It is similar to step two in that a flow diagram is developed, but this time the process improvements are incorporated. In step four the theory is operationalized as the scope of the improvement effort or plan is defined.

The "Do" phase of the model is where action step five, the pilot study, is accomplished. Here the plan or theory is carried out and tested, preferably on a small scale with the customers. The experiment may involve a change of organization or a manipulation of any of the five process resources: people, method, material, equipment, and environment.

In the "Study" phase of the PDSA model, step six of the action plan is invoked as the test results are observed. The purpose of this step is to determine if the planned

changes in the process result in a smaller gap between the Voice of the Process and the Voice of the Customer. Regardless of the outcome of this step, information is gained about the process.

In the "Act" phase of the model where the opportunity to improve the process materializes, there are two steps. In step seven, after studying the results of the pilot test, the process is improved, or it is not, by creating a new mix of the five process resources. Finally, in step eight, the PDSA Cycle starts again as the next iteration of continuous process improvement begins.

An imaginative yet enlightening illustration of the importance of the wisdom embodied in the continuous improvement PDSA model was presented in 1989 by U.S. Air Force General Loh, Commander of the Aeronautical Systems Division. He opened an address to the Modular Avionics Systems Architecture Conference with a tale from

The Christopher Robin Story Book:

Here is Edward Bear, coming downstairs now
bump,

 bump,
 bump, on the back of his head, behind
Christopher Robin. It is, as far as he knows, the only way
of coming downstairs, but sometimes he feels that there is
another way, if only he could stop bumping for a moment and
think of it.

B. Defining Foreign Ownership, Control, or Influence

In a Congressional Research Service Report on "Foreign Investment in U.S. Defense Companies," National Defense Specialist, Gary Pagliano (1992) identifies three broad types of foreign direct investment in U.S. industry. The first type of investment is when a foreign person or firm acquires ownership of 10 percent or more of the voting equity of a U.S. company. This level of ownership, as defined in the International Investment and Trade in Services Survey Act of 1974, is considered legal evidence of a long-term interest in, and a measure of influence over, the management of a company. The second type of investment is called "portfolio" investment, where foreign investors buy equity in a corporation, but hold less than 10 percent of the equity shares. Buying debt (bonds) in a U.S. company is also allowed without regulation. The third type is a catch-all for different kinds of smaller-scale investments (usually non-equity in nature) between companies such as a joint venture licensing agreement, or consortium agreement.

The Department of Defense Industrial Security Manual (DOD 5220.22-M, 1991) definition differs by placing a 5 percent threshold on equity ownership, and placing more emphasis on the national security implications of control, or influence. Specifically, factors such as foreign contracts, income from foreign interests hostile to the U.S., indebtedness to foreign interests, or the ability of foreign interest to control or influence the election,

appointment or tenure of senior company officials are considered. National security implications and the need to safeguard classified and export-controlled defense critical technologies provide ample justification for this more encompassing definition.

U
W
i
b
t
re

St
an
re
acc
tec
cur

says
Incr
indi
much
Forei

C. Defining U.S. Foreign Investment Policy

Mark Hanson, in an article in the Northwestern Journal of International Law & Business (1989) points out that in recognition of the importance of an unrestricted flow of capital, United States policy on international investment is founded upon the theory that the private market is the most efficient means to determine the allocation and use of capital in the international economy. As a result, the United States pursues an "open door" approach to investment which offers no special incentives to foreigners who invest in the United States and, in general, imposes no special barriers. Furthermore, once foreign investors establish themselves within the United States economy, they generally receive the same treatment as domestic investors.

According to Hanson, foreigners invest in the United States for a variety of reasons: the stable U.S. economic and political systems; the relative absence of government regulatory controls on business; a large consumer market; accessibility of leading-edge technology and management techniques; and finally, given the depreciating dollar, current economic conditions often make it a bargain.

Conversely, viewed from the U.S. perspective Hanson says, an open investment policy also has many benefits. Increased foreign investment helps the economy grow and individual companies to expand by providing a source for much needed capital and a conduit to the global marketplace. Foreign investment in U.S. companies also produces

employ

and ser

leads t

investm

increas

Aerospa

Decembe

have ac

able to

capital

employment opportunities, tax revenues, and consumer goods and services. Finally, an open foreign investment policy leads to reciprocity in the elimination of barriers to U.S. investment abroad. The importance of this last point in an increasingly global economy is underscored by one of the Aerospace Industries Association's key issues (AIA, 1990 December) for the 1990's which states: Our companies must have access to foreign markets on an equitable basis and be able to work with foreign partners to spread risk, raise capital, improve market access, and develop new technology.

i
p
C
or
Me
re
cre
to
for
tra
Mark

D. Defining U.S. Foreign Investment Regulations

Foreign investment in United States is subject to federal review and a number of laws and regulations which are necessary for national defense or the public welfare. Such laws and regulations include: antitrust laws; securities laws; Defense Industrial Security Program regulations; review by the Committee on Foreign Investment in the United States (CFIUS); and, in some situations, Section 5021 of the Omnibus Trade and Competitiveness Act (1988), entitled "Authority to Review Certain Mergers, Acquisitions and Takeovers" which is often referred to as the Exon-Florio Amendment. A brief description follows of all these regulations except the Defense Industrial Security Program regulations which are addressed separately, in detail.

U.S. antitrust laws (Hanson, 1989) prohibit foreign investors from obtaining an unfair aggregation of economic power which might weaken or destroy competition. The Clayton Act (1982) prevents foreign investors, acting singly or collectively, from acquiring, or participating in a merger or joint venture with a United States firm, if the result would substantially lessen competition or tend to create a monopoly. The Sherman Act (1982) may also be used to prevent acquisitions, mergers or joint ventures by foreign investors if the transactions unreasonably restrain trade or illegally attempt to monopolize a particular market. Finally the Federal Trade Commission Act (1950)

i
i
I
g
fo
Fo
re
ho
in

Uni
Pres
Depa

prohibits domestic or foreign-owned businesses from utilizing unfair methods of competition. The Hart-Scott-Rodino Antitrust Improvements Act of 1976 (1982) requires a foreign investor to notify the Justice Department and the Federal Trade Commission prior to an acquisition of voting securities, or of assets exceeding a certain amount.

The Securities Act of 1933 (1982) and the Securities and Exchange Act of 1934 (1982) require (Hanson, 1989) a foreign corporation planning to issue securities in the U.S. market, or to obtain a controlling interest in a publicly-held U.S. company, to comply with proxy rules and certain disclosure requirements. These investment disclosure requirements were expanded in the 1970's which enabled the Departments of Commerce and Treasury to oversee and regulate, but not necessarily restrict, foreign investment in the United States. Specifically, the International Investment Survey Act of 1976 (1982) resulted in the generation of more complete statistical information on foreign direct and portfolio investment. The Domestic and Foreign Investment Improved Disclosure Act of 1977 (1982) required more complete disclosure by foreign investors holding over five percent of any class of security described in Section 13(d)(1) of the Securities Exchange Act of 1934.

The interagency Committee on Foreign Investment in the United States (1975) (Hanson, 1989), created in 1975 by President Ford, consists of representatives from the Departments of State, Treasury, Defense, and Commerce, the

U.S

Adv

Tre

mon

inve

poli

fund

auth

1988

estab

or ta

provi

to na

repor

major

imple

not s

were

to wh

withi

Confe

and w

U.S. Trade Representative, and the Council of Economic Advisors. The Chair of the CFIUS is the Secretary of the Treasury. The CFIUS has primary responsibility for monitoring the impact of direct and portfolio foreign investment and for coordinating the implementation of U.S. policy on such investment. Discretionary review is the fundamental authority vested in the CFIUS for it has no authority to administer any laws or regulations.

The CFIUS (Pagliano, 1992) process was strengthened in 1988, when Congress passed the Exon-Florio Amendment. It established a process to investigate mergers, acquisitions, or takeovers of a U.S. company by foreign investors and provided the President authority to block a transaction due to national security considerations. Olin Wethington (1991) reported that the definition of "national security" was the major theme of public comments received on regulations implementing Exon-Florio during the summer of 1989. While not specifically defining it, the final regulations which were promulgated in November 1991 suggest the judgement as to whether a transaction threatens national security rests within the President's discretion. Further, a Congressional Conference Report suggests it is to be interpreted broadly and without limitation to particular industries.

E.

the

regu

(DIS)

Execu

Class

Secur

5220.

DISP

behal

agenci

classi

Invest

been d

conduc

securi

evolve

Secret

along

respon

unique

D

5220.2

tion, I

Securi

E. Defining the Evolution of Defense Industrial Security Program Foreign Ownership, Control, or Influence Security Regulations

Another method to control foreign direct investment in the defense industrial base exists within the implementing regulations of the Defense Industrial Security Program (DISP) which was established pursuant to Presidential Executive Order 10865 (1960, February 20) Safeguarding Classified Information Within Industry, and the National Security Act (1947). The Department of Defense (DOD ISM 5220.22-M, 1991, January) is the Executive Agent for the DISP and the Secretary of Defense is authorized to act on behalf of twenty other Executive Branch departments and agencies in providing security services to safeguard classified information entrusted to industry. The Defense Investigative Service (DIS) of the Department of Defense has been delegated responsibility by the Secretary of Defense to conduct personnel security investigations and industrial security oversight. A similar arrangement is expected to evolve in the NISP (NISP Report, September 1991) however the Secretary of Energy, the Director of Central Intelligence, along with the Nuclear Regulatory Commission will be responsible for the administration of security matters unique to their statutory authority.

DISP security regulations are promulgated in Directive 5220.22-R (1985, December) the Industrial Security Regulation, Directive 5220.22-M (1991 January), the Industrial Security Manual for Safeguarding Classified Information,

al
The
fac
uni
aut
inf
fac
firm
clas
orga
or P
a se
441
the c
contr
infor

must
(FOC
clear
It is
exist
such
opera
infor
contr
by a

along with a variety of other related security regulations. These regulations provide for the establishment of a facility security clearance to allow industrial firms, universities, or other organizations sponsored by an authorized government agency, to access national security information when performing on classified contracts. A facility clearance is an administrative determination that a firm is eligible, from a security viewpoint, for access to classified information. The firm must be located in, and organized under the laws of any of the fifty United States or Puerto Rico. As part of the facility clearance process, a senior management official of the firm executes a DD Form 441 "Department of Defense Security Agreement" on behalf of the company. The Security Agreement (Figure 2.3) is a contract wherein the firm agrees to safeguard classified information in accordance with DOD ISM 5220.22-M.

Furthermore, DoD regulations (1991) state that the firm must not be under foreign ownership, control, or influence (FOCI) to such a degree that the granting of a facility clearance would be inconsistent with the national interest. It is considered to be under FOCI when a reasonable basis exists to conclude that the nature and extent of FOCI is such that foreign dominance over its management and operations may result in the compromise of classified information or adversely impact performance on classified contracts. A firm that is owned, controlled, or influenced by a foreign national or a commercial or governmental entity

DEPARTMENT OF DEFENSE SECURITY AGREEMENT	Form Approved OMB No. 0704-0194 Expires Jul 31, 1993
---	--

Public reporting burden for this collection of information is estimated to average 14 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0194), Washington, DC 20503. Please DO NOT RETURN your form to either of these addresses. Send your completed form to your respective Cognizant Security Office.

This DEPARTMENT OF DEFENSE SECURITY AGREEMENT (hereinafter called the Agreement), entered into this _____ day of _____, 19____, by and between THE UNITED STATES OF AMERICA through the Defense Investigative Service acting for the Department of Defense and other governmental User Agencies (hereinafter called the Government), and _____ (hereinafter called the Contractor), which is:

(1) a corporation organized and existing under the laws of the state of _____

(2) a partnership consisting of _____

(3) an individual trading as _____

with its principal office and place of business at (Street, city, state and ZIP code) _____

WITNESSETH THAT:

WHEREAS, the Government has in the past purchased or may in the future purchase from the Contractor supplies or services, which are required and necessary to the national security of the United States; or may invite bids or request quotations on proposed contracts for the purchase of supplies or services, which are required and necessary to the national security of the United States; and

WHEREAS, it is essential that certain security measures be taken by the Contractor prior to and after being accorded access to classified information; and

WHEREAS, the parties desire to define and set forth the precautions and specific safeguards to be taken by the Contractor and the Government in order to preserve and maintain the security of the United States through the prevention of improper disclosure of classified information, sabotage, or any other acts detrimental to the security of the United States:

NOW, THEREFORE, in consideration of the foregoing and of the mutual promises herein contained, the parties hereto agree as follows:

Section I - SECURITY CONTROLS

(A) The Contractor agrees to provide and maintain a system of security controls within the organization in accordance with the requirements of the Department of Defense "Industrial Security Manual for Safeguarding Classified Information" (hereinafter called the Manual) attached hereto and made a part of this agreement, subject, however, (i) to any revisions of the Manual required by the demands of national security as determined by the Government, notice of which shall be furnished to the Contractor, and (ii) to mutual agreements entered into by the parties in order to adapt the Manual to the Contractor's business and necessary procedures thereunder. In order to place in effect such security controls, the Contractor further agrees to prepare Standard Practice Procedures for internal use, such procedures to be consistent with the Manual. In the event of any inconsistency between the Manual, as revised, and the Contractor's Standard Practice Procedures, the Manual shall control.

(B) The Government agrees that it shall indicate when necessary, by security classification (TOP SECRET, SECRET, or CONFIDENTIAL), the degree of importance to the national security of information pertaining to supplies, services, and other matters to be furnished by the Contractor to the Government or by the Government to the Contractor, and the Government shall give written notice of such security classification to the Contractor and of any subsequent changes thereof; provided, however, that matters requiring security classification will be assigned the least restricted security classification consistent with proper safeguarding of the matter concerned, since over-classification causes unnecessary operational delays and depreciates the importance of correctly classified matter. Further, the Government agrees that when Atomic Energy information is involved it will, when necessary, indicate by a marking additional to the classification marking that the information is "RESTRICTED DATA." The "Department of Defense Contract Security Classification Specification" (DD Form 254) is the basic document by which classification, regrading, and declassification specifications are documented and conveyed to the Contractor.

(C) The Government agrees, on written application, to grant personnel security clearances to eligible employees of the Contractor who require access to information classified TOP SECRET, SECRET, or CONFIDENTIAL.

(D) The Contractor agrees to determine that any subcontractor, subbidder, individual, or organization proposed for the furnishing of supplies or services which will involve access to classified information, has been granted an appropriate Department of Defense facility security clearance, which is still in effect prior to according access to such classified information.

Section II - INSPECTION

Designated representatives of the Government responsible for inspection pertaining to industrial plant security shall have the right to inspect, at reasonable intervals, the procedures, methods, and facilities utilized by the Contractor in complying with the requirements of the terms and conditions of the Manual. Should the Government, through its authorized representative, determine that the Contractor's security methods, procedures, or facilities do not comply with such requirements, it shall submit a written report to the Contractor advising of the deficiencies.

Figure 2.3
Department of Defense Security Agreement
DD Form 441 (Page 1 of 2)

Section III - MODIFICATION

Modification of this Agreement may be made only by written agreement of the parties hereto. The Manual may be modified in accordance with section I of this Agreement.

Section IV - TERMINATION

This agreement shall remain in effect until terminated through the giving of 30 days written notice to the other party of intention to terminate; provided, however, notwithstanding any such termination, the terms and conditions of this Agreement shall continue in effect so long as the Contractor possesses classified information.

Section V - PRIOR SECURITY AGREEMENTS

As of the date hereof, this Agreement replaces and succeeds any and all prior security or secrecy agreements.

understandings, and representations with respect to the subject matter included herein entered into between the Contractor and the Government, provided that the term "security or secrecy agreements, understandings, and representations" shall not include agreements, understandings, and representations contained in contracts for the furnishing of supplies or services to the Government which were previously entered into between the Contractor and the Government.

Section VI - SECURITY COSTS

This agreement does not obligate Government funds, and the Government shall not be liable for any costs or claims of the Contractor arising out of this Agreement or instructions issued hereunder. It is recognized, however, that the parties may provide in other written contracts for security costs, which may be properly chargeable thereto.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the day and year written above:

THE UNITED STATES OF AMERICA

By _____

(Authorized Representative of the Government)

(Contractor)

By _____

(Title)

(Contractor)

(Address)

WITNESS

NOTE: In case of a corporation, a witness is not required but the certificate must be completed. Type or print names under all signatures.

NOTE: Contractor, if a corporation, should cause the following certificate to be executed under its corporate seal, provided that the same officer shall not execute both the Agreement and the Certificate.

CERTIFICATE

I, _____, certify that I am the _____

of the corporation named as Contractor herein; that _____

who signed this agreement on behalf of the Contractor, was then _____ of said corporation; that said agreement was duly signed for and in behalf of said corporation by authority of its governing body, and is within the scope of its corporate powers.

(Corporate Seal)

(Signature and Date)

DD Form 441 Reverse, JUL 90

Figure 2.3
Department of Defense Security Agreement
DD Form 441 (Page 2 of 2)

whose interests are inimical to the U.S. is not eligible for a facility clearance. However, firms whose FOCI does not derive from such hostile sources may be eligible for a clearance provided action can be taken to effectively negate or reduce associated FOCI security risks to an acceptable level.

Compared to other departments and agencies of the Executive Branch, DoD security regulations (5220.22-R and 5220.22-M) addressing FOCI are the most mature. The primary factors considered by DoD in determining whether firms are under FOCI are identified in the DD Form 441S "Certificate Pertaining to Foreign Interests" (Figure 2.4) which must be completed by the firm as part of the facility clearance determination process and updated whenever conditions related to FOCI change such that it affects the information previously reported.

DoD regulations (1991) provide that, if the DIS determines that any of the FOCI factors identified in the 441S are present, the case will be reviewed to determine the relative significance of each factor in assessing the firm's initial or continuing eligibility for a facility clearance. If a firm under FOCI may be ineligible for a facility clearance, or additional action would be necessary to nullify or negate the effects of FOCI, the firm will be so advised by the DIS and requested to submit a plan to preclude foreign access to classified information. If an acceptable plan is not submitted, facility clearance processing is

CERTIFICATE PERTAINING TO FOREIGN INTERESTS		Form Approved OMB No. 0704-0024 Expires Aug 31, 1993
(Type or print all answers)		
Public reporting burden for this collection of information is estimated to average 78 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0024), Washington DC 20503. Please DO NOT RETURN your form to either of these addresses. Send your completed form to your respective Cognizant Security Office.		
PENALTY NOTICE		
<p>Failure to answer all questions or any misrepresentation (by omission or concealment, or by misleading, false or partial answers) may serve as a basis for denial of clearance for access to classified Department of Defense information. In addition, Title 18, United States Code 1001, makes it a criminal offense, punishable by a maximum of five (5) years imprisonment, \$10,000 fine, or both,</p>	<p>knowingly to make a false statement or representation to any Department or Agency of the United States, as to any matter within the jurisdiction of any Department or Agency of the United States. This includes any statement made herein which is knowingly incorrect, incomplete or misleading in any important particular.</p>	
PROVISIONS		
<p>1. This report is authorized by the Secretary of Defense pursuant to authority granted by Executive Order 10865. While you are not required to respond, your eligibility for a facility security clearance cannot be determined if you do not complete this form. The retention of a facility security clearance is contingent upon your compliance with the requirements of DoD 5220.22-M for submission of a revised form as appropriate.</p>	<p>2. When this report is submitted in confidence and is so marked, applicable exemptions to the Freedom of Information Act will be invoked to withhold it from public disclosure.</p> <p>3. Complete all questions on this form. Mark "Yes" or "No" for each question. If your answer is "Yes" furnish in full the complete information under "Remarks."</p>	
QUESTIONS AND ANSWERS		
1. Do foreign interests own or have beneficial ownership in 5% or more of your organization's securities?	YES	NO
2. Does your organization own any foreign interest in whole or in part?		
3. Do any foreign interests have positions, such as directors, officers, or executive personnel in your organization?		
4. Does any foreign interest control or influence, or is any foreign interest in a position to control or influence the election, appointment, or tenure of any of your directors, officers, or executive personnel?		
5. Does your organization have any contracts, agreements, understandings or arrangements with a foreign interest(s)?		
6. Is your organization indebted to foreign interests?		
7. Does your organization derive any income from designated countries or income in excess of 10% of gross income from non-designated foreign interests?		
8. Is 5% or more of any class of your organization's securities held in "nominee shares," in "street names" or in some other method which does not disclose the beneficial owner of equitable title?		
9. Does your organization have interlocking directors with foreign interests?		
10. Are there any citizens of foreign countries employed by or who may visit your facility (or facilities) in a capacity which may permit them to have access to classified information?		
11. Does your organization have any foreign involvement not otherwise covered in your answers to the above questions?		

DD Form 441S, AUG 90

Previous editions are obsolete.

Figure 2.4
Department of Defense
Certificate Pertaining to Foreign Interests
DD Form 441S (Page 1 of 3)

I CERT
knowledg

WITNESS:

NOTE: In case
certificate be
under all signat

NOTE: Contr
same

I _____
of the corp
who signed
of said corp
authority of

REMARKS (Attach additional sheets, if necessary, for a full detailed statement.)	
CERTIFICATION	
<p>I CERTIFY that the entries made by me above are true, complete, and correct to the best of my knowledge and belief and are made in good faith.</p> <p>WITNESS:</p> <div style="display: flex; justify-content: space-between; margin-top: 20px;"> <div style="width: 45%;"> <p>_____</p> <p>_____</p> </div> <div style="width: 50%;"> <p>_____ (Date Certified)</p> <p>By _____</p> <p>_____ (Contractor)</p> <p>_____ (Title)</p> <p>_____ (Address)</p> </div> </div>	
<p>NOTE: In case of corporation, a witness is not required but certificate below must be completed. Type or print names under all signatures.</p>	
<p>NOTE: Contractor, if a corporation, should cause the following certificate to be executed under its corporate seal, provided that the same officer shall not execute both the agreement and the certificate.</p>	
CERTIFICATE	
<p>I, _____, certify that I am the _____ of the corporation named as Contractor herein; that _____ who signed this certificate on behalf of the Contractor, was then _____ of said corporation; that said certificate was duly signed for and in behalf of said corporation by authority of its governing body, and is within the scope of its corporate powers.</p> <div style="display: flex; justify-content: space-between; margin-top: 20px;"> <div style="width: 45%; text-align: center;"> <p>_____</p> <p>(Corporate Seal)</p> </div> <div style="width: 50%; text-align: center;"> <p>_____</p> <p>(Signature and Date)</p> </div> </div>	

DD Form 441S Reverse, AUG 90

Figure 2.4
Department of Defense
Certificate Pertaining to Foreign Interests
DD Form 441S (Page 2 of 3)

in co
conu
subn

QUE
fore
Sche
attac

QUES
of off

QUES
or she

QUEST

QUEST
Agreen
ventur
the SEC

QUEST
of the c
voting
furnish

QUEST
percent
involved
and typ
identify

QUEST
identific
whether
the appo
have atte
the inves

QUEST
Also, ind

QUEST
are a citi
included

QUEST
reportable

INSTRUCTIONS FOR COMPLETING THE DD FORM 441s

In completing the DD Form 441s, all items are to be answered by indicating X in either the YES or NO column. If an answer to any question is YES, the following paragraphs provide instructions for the submission of the necessary data.

QUESTION 1. Identify the percentage of any class of shares or other securities issued, that is owned by foreign interests, broken down by country. If the answer is YES and a copy of Schedule 13D and/or Schedule 13G filed by the investor with the Securities and Exchange Commission (SEC), has been received, attach a copy to the revised DD Form 441s.

QUESTION 2. Furnish the name, address by country, and the percentage owned. Include name and title of officials of the facility who occupy positions with the foreign entity, if any.

QUESTION 3. Furnish full information concerning the identity of the foreign interest, and the position he or she holds in the organization.

QUESTION 4. Identify the foreign interest(s) and furnish full details concerning the control or influence.

QUESTION 5. Furnish name of foreign interest, country, and nature of agreement or involvement. Agreements include licensing, sales, patent exchange, trade secrets, agency, cartel, partnership, joint venture, and proxy. If the answer is YES and a copy of Schedule 13D and/or 13G filed by the investor with the SEC has been received, attach a copy to the revised DD Form 441s.

QUESTION 6. Furnish the amount of indebtedness and by whom furnished as related to the current assets of the organization. Include specifics as to the type of indebtedness and what, if any, collateral, including voting stock, has been furnished or pledged. If any debentures are convertible, specifics are to be furnished.

QUESTION 7. State full particulars with respect to any income from Designated countries, including percentage from each such country, as related to total income, and the type of services or products involved. If income is from non-designated countries, give overall percentage as related to total income and type of services or products in general terms. If income is from a number of foreign countries, identify countries and include percentage of income by each country.

QUESTION 8. Identify each foreign institutional investor holding 5 percent or more of the voting stock. Identification should include the name and address of the investor and percentage of stock held. State whether the investor has attempted to, or has in fact, exerted any management control or influence over the appointment of directors, officers, or other key management personnel, and whether such investors have attempted to influence the policies of the corporation. If a copy of Schedule 13D and/or 13G filed by the investor with the SEC has been received, attach a copy to the revised DD Form 441s.

QUESTION 9. Include identifying data on all such directors. If they have a security clearance, so state. Also, indicate the name and address of all other corporations with which they serve in any capacity.

QUESTION 10. Provide complete information by identifying the individuals and the country of which they are a citizen. Foreign visitors, officially sponsored by a foreign government or User Agency, are not included in the range of this question.

QUESTION 11. Describe the foreign involvement in detail, including why the involvement would not be reportable in the preceding questions.

ter

DoD

dec

mit

sec

fore

thre

of w

by-ca

subje

discr

Direct

an eve

has be

cases.

ment,

From i

been g

viable

U.S. or

De

under no

under co

concern v

sufficien

terminated or an existing facility clearance is revoked. DoD provides an appeal process for termination or revocation decisions and will work with the firm to modify the FOCI mitigation plan until it adequately protects national security interests.

Hanson (1989) points out that the greatest obstacle to foreign investment in the defense industry is passing the threshold test for FOCI. There is no standard determination of what constitutes FOCI, and decisions are made on a case-by-case basis. Ultimately, the determination of FOCI is a subjective evaluation, in which the DIS has substantial discretionary authority.

Several FOCI mitigation instruments are detailed in DoD Directive 5220.22-M. These security solutions demonstrate an evolution of policy over more than thirty years, which has been the DoD's response to increasingly complex FOCI cases. In general, policy changes were prompted by government, industry, or situational demands for flexibility. From its inception, DoD FOCI security policy appears to have been guided by an understanding of the criticality of a viable defense industrial base, and the need for access to U.S. or foreign-owned leading-edge technology.

Department of Defense regulations (1991) state that under normal circumstances, foreign ownership of a U.S. firm under consideration for a facility clearance becomes a concern when the amount of foreign-owned stock is at least sufficient to elect representation to the U.S. firm's Board

of Dir
positi
applie
Foreig
itself
Board

De
when tl
control
the Bo
allowed
mitigat
firm mu
continu
The res
represe
it must
exclude
and fro
the fir
classif
chief e
interes
citizens
such arr
monitore
As neces

of Directors or foreign interests are otherwise in a position to select such representatives. This standard also applies to equivalent equity for an unincorporated business. Foreign ownership which is not so manifested is not, in itself, considered significant.

Board Resolutions

Department of Defense regulations (1991) suggest that when the amount of stock owned by a foreign interest is not controlling, but is sufficient to elect representation to the Board, or a representative of a foreign interest is allowed to sit on the Board, the effects of FOCI may be mitigated by a "Resolution of the Board of Directors." The firm must first acknowledge the FOCI, and second, its continuing obligations under the DoD 441 Security Agreement. The resolution must identify the foreign shareholders, their representatives, and the extent of ownership. Additionally, it must certify that the foreign interest can be effectively excluded from access to government classified information, and from any positions which would enable them to influence the firm's policies and practices in performing on classified contracts. Further, the company chairperson and chief executive officer must be U.S. citizens, the foreign interest can not be the largest single shareholder, and U.S. citizens must own a majority of the stock. Compliance with such arrangements, which date back to the 1950s, is monitored by the DIS during facility security inspections. As necessary, the Board may be required to implement

add

res

cons

Reci

anot

facil

estab

(GSOI

agree

betwe

inform

standa

develop

militar

Recipro

influen

for acc

consist

agreemen

granting

of one c

Facility

governmen

firm has

nation's s

additional administrative controls or adopt further resolutions to ensure the facility clearance remains consistent with the national interest.

Reciprocal Facility Clearances

Department of Defense regulations (1991) provide another FOCI mitigation instrument called a "Reciprocal" facility security clearance, a solution which stems from established General Security of Information Agreements (GSOIA) between the U.S and certain allied nations. These agreements facilitate the exchange of classified information between cooperating countries, and the safeguarding of such information in accordance with mutually acceptable standards. The Reciprocal security clearance concept was developed in the 1960's in response to co-production military programs between the U.S. and Canada. The Reciprocal clearance allows a firm owned, controlled, or influenced by investors from an allied nation to be eligible for access to the other nation's classified information consistent with the terms of the government-to-government agreement. These arrangements also provide a method for granting personnel security clearances to foreign nationals of one country employed by a firm in the other country. Facility clearance processing requires the transmittal of a government-to-government security assurance that the parent firm has been cleared to the necessary level under that nation's security regulations.

Votin

Agree

encou

Votin

elim

of the

owns

that t

contro

manage

title

truste

have h

invest

preroge

fiducia

and hav

without

investo

terms o

limited

company.

authorit

investor

a signif

or other

Voting Trust Agreements

The Department of Defense developed the Voting Trust Agreement in 1968 to isolate a parent company when it encountered the first 100% foreign ownership case. The Voting Trust has evolved into an acceptable method to eliminate FOCI risks when a foreign interest owns a majority of the voting securities of a cleared U.S. firm, or if it owns less than 51% of the stock but it can be determined that the foreign interest is in a position to effectively control, or have a dominant influence over, the business management of the firm. In a Voting Trust Agreement, legal title of foreign-owned stock is transferred to U.S. citizen trustees who are approved by the DIS. The trustees must not have had any prior affiliation with either the foreign investor or the cleared U.S. firm, and must be provided all prerogatives of stock ownership. Trustees accept a fiduciary responsibility, a DoD security "watchdog" role, and have the complete freedom to act independently and without consultation with, or interference by, the foreign investor. The investor derives the benefits of ownership in terms of profit or stock dividends, but otherwise has only limited input into the management or operations of the company. The Voting Trust Agreement may limit the authorities of the Trustees by requiring the foreign investor's approval for such transactions as: sale of all or a significant part of the firm's assets; pledges, mortgages or other encumbrances on the capital stock held in trust by

the

corp

the

busin

inde

Proxy

creat

subst

the P

trans

stock

accomp

inter

invest

Speci

R

the vo

contro

relinq

be gra

or SSA

used i

invest

of a cl

U.S. co

designe

the foreign investors; mergers, consolidations, or major corporate reorganizations; dissolution of the company; or the filing of a bankruptcy petition. The cleared U.S. business must be organized and financed to function independent from the foreign interest.

Proxy Agreements

The Voting Trust concept was modified in the 1970's by creation of the Proxy Agreement. The terms of the Proxy are substantially the same as the Voting Trust except that under the Proxy the voting rights of the foreign-owned stock are transferred to Proxy Holders, however, legal title to the stock remains with the foreign interests. This arrangement accomplishes the same level of isolation between the foreign interest and the U.S. firm, and is more palatable to the investor.

Special Security Agreements

Finally, when a foreign interest acquires a majority of the voting stock of a cleared U.S. firm, or effectively controls its management or operations and refuses to relinquish that control, a facility security clearance may be granted under the terms of a Special Security Agreement, or SSA. The SSA concept was developed in 1984 and has been used in certain situations to grant a majority foreign investor minority representation on the Board of Directors of a cleared U.S. firm. The SSA is an agreement among the U.S. company, the foreign interest, and the DoD. It is designed to mitigate or limit the potential for disclosure

of c

adve.

the

tail

prese

Agree

FOCI

class

secur

direct

Truste

"Offic

serve

board.

securi

which

"Insid

classi

DSC ma

Proxy.

lower a

accompl

governm

a policy

agency w

other hi

of classified or other export-controlled information, or for adverse management impact exercised by a foreign interest on the U.S. operation.

Security countermeasures incorporated into an SSA are tailored to the risk and the nature and extent of FOCI present in the case. Minimally, a Reciprocal Security Agreement must be in place with the nation from which the FOCI emanates, and only U.S. citizens are allowed access to classified information in connection with the facility security clearance. A number of U.S. citizen "Outside" directors function in a watchdog capacity similar to the Trustee or Proxy Holder. Additionally, U.S. citizen "Officer" directors operationally manage the business and serve as a liaison between the cleared company and the board. Outside and Officer directors, along with the security officer, form a Defense Security Committee (DSC), which ensures security and export regulation compliance. "Inside" directors representing the parent are excluded from classified or export-restricted discussions of the board. A DSC may be formed in a firm cleared under a Voting Trust or Proxy. An SSA is generally granted at the SECRET level or lower after a National Interest Determination (NID) is accomplished by DoD security officials and the contracting government agency. On occasion, based on demonstrated need, a policy waiver may be granted by an authorized government agency which allows the U.S. firm access to TOP SECRET, or other highly sensitive classified material.

DISP

Frenc

acqu:

LTV (

11 ba

\$280

with

bid \$

the L'

of Gen

the m.

indica

Depart

clear:

contra

"show

Thoms

busine

Corpor

it was

to \$45

The U.

expect

govern

F. Globalization Future Shock
Thomson CSF Attempts to Acquire LTV

Perhaps the most significant test of the quality of DISP FOCI security regulations came in April 1992, when the French-owned company Thomson CSF made a controversial bid to acquire part of the assets of the U.S. defense contractor LTV (Pearlstein, 1992, April 19) which had been in Chapter 11 bankruptcy-court proceedings since 1986. Thomson offered \$280 million for LTV's missile division in a joint effort with a Washington investment firm, the Carlyle Group, who bid \$90 million cash and \$30 million in preferred stock for the LTV aerospace division. Hughes Aircraft Corp., a unit of General Motors Corp., also agreed to buy a 15% stake in the missile business. The Thomson/Carlyle team later indicated that it had received assurances from Defense Department officials that Thomson could receive security clearance to work on the bulk of LTV's army missile contracts, and that they had been advised there were no "show stoppers" to a Thomson bid. The \$400 million total Thomson/Carlyle offer topped a \$355 joint offer for the business from the U.S.-owned Lockheed and Martin Marietta Corporations, and started a high stakes bidding war. Before it was over the foreign-led investors increased their offer to \$450 million with a \$20 million non-refundable deposit. The U.S. partners increased their bid to \$385 million fully expecting the French offer would not receive the requisite government approval. The decision by a New York bankruptcy

judge

Lockhe

played

T

indust

Congre

nation

Wall S

Thomson

manufac

someday

Thomson

evaluat

judge's

into fo

governm

recent

the Pre

tion ha

governm

were ov

Se

sophist.

known to

informat

Special

over the

judge to accept the Thomson/Carlyle bid enraged the Lockheed/Martin Marietta team and sparked a controversy that played out in Congressional hearings and the news media.

The Thomson deal, a significant step toward defense industry globalization, shocked and concerned many in Congress and the Executive Branch because of the acute national security considerations inherent in the deal. The Wall Street Journal (Hayes, 1992, April 6) portrayed the Thomson bid as triggering fears that the sale of a missile manufacturing business (LTV) to a foreign concern would someday come back to haunt the U.S. government. As the Thomson/Carlyle offer moved through the regulatory evaluation process in the weeks following the bankruptcy judge's decision to accept the bid, three threat issues came into focus. First, attention centered on the French government's ownership of 58% of Thomson CSF. Given a recent national television disclosure by the retired head of the French foreign intelligence service that his organization had been spying on U.S. industry for years, many in government and the private sector speculated that the French were overtly attempting to steal U.S. missile technology.

Second, as a major defense firm involved in sophisticated aerospace and missile technology, LTV was known to possess large amounts of highly classified information. The French made it clear that they wanted a Special Security Agreement in order to have some control over the management and operations of their multi-million

dollar

holding

Restrict

category

firm, c

T

by a c

Caroli

Chairm

Brady

outlaw

the de

govern

a nat

Week a

Custor

diver

stati

by re

the T

the s

Defens

nation

both H

to enh

U

designe

dollar investment. The significant percentage of classified holdings at LTV in the TOP SECRET, Restricted Data, Formerly Restricted Data, COMSEC, and Special Access Program categories, which are normally off limits to an SSA cleared firm, quickly became a point of contention.

The third threat issue in the case was best summarized by a comment (Wartzman, 1992, November 2) written by South Carolina Democratic Senator, and Commerce Committee Chairman, Ernest Hollings to Treasury Secretary Nicholas Brady warning that Thomson "has a record of selling arms to outlaw regimes." Indeed part of the controversy surrounding the deal, highlighted by the Senator's allegation, was the government's ability to accurately quantify the threat from a national security intelligence perspective. A Business Week article (1992, July 20) cited a July 2 report that the Customs Service was investigating whether Thomson illegally diverted U.S. lasers to Iraq. Thomson denied the charge, stating the lasers were French-made and the sales approved by regulators in Paris. In any case, the Senate condemned the Thomson deal in a nonbinding resolution, 93-4. Later in the summer, acting on the work of the fiscal year 1993 Defense Authorization Conference findings that found FOCI national security intelligence gathering efforts lacking, both Houses of Congress passed legislation (Tolchin, 1992) to enhance FOCI data collection and risk assessment.

Ultimately, DISP FOCI security regulations worked as designed and Thomson CSF was forced to accept a Voting Trust

or P

safe

LTV.

who v

witho

(Silv

to Lo

partn

Los A

or Proxy arrangement as the only acceptable means of safeguarding the sensitive technology in the possession of LTV. This ruling proved to be a deal-breaker for the French who were ultimately able to back out of the deal gracefully without losing their sizeable deposit. LTV was later split (Silverberg, 1992, August) as the missile business was sold to Loral in New York and the aerospace business to a new partnership formed between the Carlyle Group and Northrop in Los Angeles.

III.

for

tion

of th

to hi

Presi

provi

and i

such

includ

author

of an

FOCI

objec

Presi

FOCI

impac

review

was pe

evalua

A

governm

the mer

rational

III. METHODOLOGY - DEMING'S CYCLE: PLAN, DO, STUDY, ACT

A. "Plan" Step One: Identification of the Opportunity for Improvement

The first part of the Deming Cycle calls for a "Plan" for process improvement. Scherkenbach's (1991) interpretation of this phase suggests step one involves a comparison of the Voice of the Customer with the Voice of the Process to highlight the variance or gap between the two voices. President Bush's 1991 endorsement of the NISP concept provided an opportunity to create an interagency government and industry forum of security professionals to accomplish such a comparison on all industrial security policy, including that pertaining to FOCI situations. Granted the authority to take a clean slate approach in the development of an Executive Branch standard, the International Security FOCI Working Group indicated progress toward its stated objectives in the 1991 NISP Report (Atwood, et al.) to the President. Not surprisingly though, media scrutiny of DISP FOCI security regulations in the wake of Thomson CSF/LTV impacted the NISP FOCI Working Group efforts to critically review the current Voice of the Process. Thomson's effect was perhaps even more significant than the mood for process evaluation and improvement originally generated by the NISP.

After the Thomson case, it became a challenge for government policymakers to set aside opposing convictions on the merits of foreign direct investment and move toward a rational security policy for foreign ownership, control, or

influen

is a c

titled

Assist

Securi

design

FOCI s

policy

nation

straw

Voting

highli

the Vo

T

Voice

effect

Proces

Depart

of sec

varyin

has ac

the Sp

While i

often v

countern

Voting T

arrangeme

influence of defense firms in the NISP. One example of this is a controversial August 28, 1992 memorandum (Stewart) titled, "Interim guidance on FOCI Cases" from the Deputy Assistant Secretary of Defense, Counterintelligence and Security Countermeasures. Later described as a "strawman" designed to stimulate dialogue in charting the future of FOCI security policy, the memo suggested a very restrictive policy trend that many in government, industry, and foreign nations found unworkable. The controversy surrounding the strawman policy, which advocated broader application of the Voting Trust/Proxy isolation methodology, did however highlight the variance between the Voice of the Customer and the Voice of the Process as illustrated in Figure 3.1.

The Voice of the Customer is quite clear, it is the Voice of the NISP that calls for an efficient and cost-effective, threat driven security program. The Voice of the Process is unfortunately less clear. Despite Defense Department attempts over thirty years to develop a variety of security countermeasure solutions which respond to varying levels of FOCI threat, in recent years the Process has actually developed two distinct and competing voices, the Special Security Agreement and the Voting Trust/Proxy. While in many ways these two voices are similar, they are often viewed as polar extremes. An "either/or" security countermeasures situation has seemingly developed. The Voting Trust or Proxy is seen by some as a perfect security arrangement because it isolates the foreign parent from the

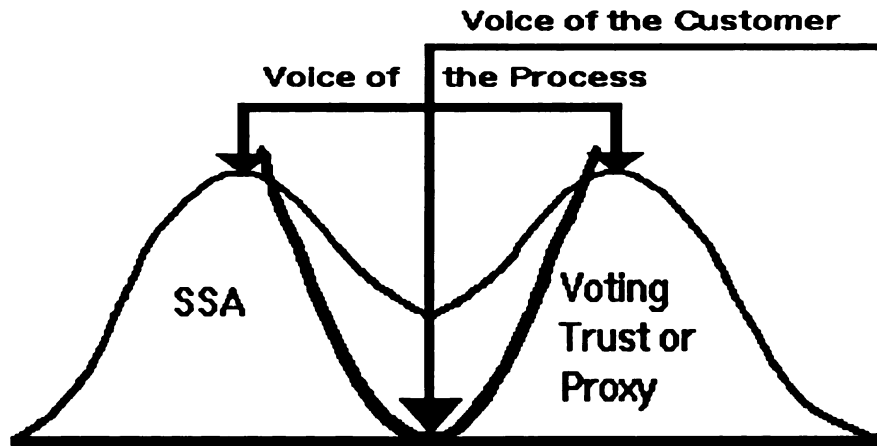


Figure 3.1

The Voice of the Customer (NISP) versus the two current Voices of the Process (SSA or Trust/Proxy)
 (An adaptation of Scherkenbach, 1991, p. 78)

cleared U.S. subsidiary. The SSA, on the other hand, has developed an undeserved stigma as a technology sieve because it only insulates the subsidiary and is designed to mitigate or limit the potential for adverse management impact exercised by the foreign parent on classified or export-controlled technology. Thus, in the minds of some policymakers and administrators, either a Voting Trust/Proxy is implemented, or little has been done about the FOCI threat. This is an unfortunate circumstance because, reiterating the statement in the 1990 NISP (Atwood et al.) report:

the globalization of industry, coupled with increased economic competition and dramatic strategic developments in East-West relations, will lead to new and different threats from both old and new adversaries.

Pol

the Pro

develop

in a st

Committ

militar

do not

to a P

indica

mitiga

GAO st

(no ci

negate

C

Office

and be

classi

govern

demons

securi

Defens

servic

classi

Voting

on live

The rea

appears

Policymakers might dispute the idea of two Voices of the Process; however, evidence of their existence was developed by the General Accounting Office (1990, March 21) in a statement prepared for the House of Representatives, Committee on Armed Services. The GAO stated that some military service and Defense Investigative Service officials do not agree that an SSA is a fully acceptable alternative to a Proxy or Voting Trust Agreement. Each service indicated that SSAs are the least desirable method to mitigate FOCI and should be used only as a last resort. The GAO statement also referenced a 1989 Army policy memorandum (no citation provided) that stated: because an SSA does not negate FOCI it can only be used when all other means fail.

Conversely, GAO stated that some officials from the Office of the Secretary of Defense do not share these views and believe that SSAs provide adequate protection for classified material. The lack of empirical data in the government to justify skepticism about SSAs was also demonstrated in the GAO inquiry. GAO indicated that security officials from the Office of the Secretary of Defense, the Defense Investigative Service, and the military services said they were not aware of any compromises of classified data under SSAs. In the final analysis, the Voting Trust/Proxy and SSA alternatives seem to have taken on lives of their own, partly based on fact, mostly on myth. The real issue, as evidenced elsewhere in the GAO testimony, appears to be a widespread lack of understanding of FOCI

security

circums

appropri

material

Gi

Process

for FOI

First,

opportu

counter

looking

of the

method

of the

creati

that i

In oth

must b

securi

ways,

T

is inte

the Pro

opportu

tailor t

threat i

efficien

security countermeasures, and a need to clarify the circumstances under which an SSA is acceptable or appropriate, particularly for protecting highly classified material.

Given the reality of two FOCI security countermeasure Process Voices, there are actually two major opportunities for FOCI security countermeasures process improvement. First, given the dynamic threat environment, there is the opportunity to encourage those involved in FOCI security countermeasures planning for the NISP to take a more forward looking approach to their efforts. This entails elimination of the total reliance on past or present threat abatement methods and the preoccupation with the two dominant Voices of the Process, the SSA and Voting Trust/Proxy. A menu of creative approaches should replace the "either/or" mentality that inhibits progress on this complex security challenge. *In other words, the range of security countermeasure options must be flexible enough to adapt to the multiplicity of FOCI security threats which manifest themselves in different ways, and in varying degrees of seriousness.*

The second opportunity for process improvement, which is integral to the first, involves alignment of the Voice of the Process with the Voice of the Customer. This opportunity is really a restatement of the NISP goal to tailor the security countermeasures process to the level of threat inherent in each case, and to do so in the most efficient and cost-effective manner. This necessitates

deve

coun

thre

Sche

is c

development of a graduated scale of threat driven security countermeasures applicable to increasingly complex FOCI threat scenarios. The end product as Deming and Scherkenbach suggest, is a single Voice of the Process that is clear and aligned with the Voice of the Customer.

B.

Plan

docu

diag

make

inef

modi

the)

Voic

Progr

strai

is pr

DoD s

"Cert

as th

repor

speci

name,

inter

must

by le

protec

exempt

the cl.

B. "Plan" Step Two: Documenting the Present Process in a Critical Examination of FOCI Security Regulations

According to Scherkenbach (1991), in step two of the Plan phase of the Deming Cycle the present process is documented, preferably in the form of a process flow diagram. A graphical representation of the existing process makes it easier to spot parts of the process that are inefficient or ineffective, and therefore lend themselves to modification or simplification. The problems identified in the process flow model relate to the variance between the Voice of the Process and the Voice of the Customer.

An illustration of the Defense Industrial Security Program FOCI adjudication process model which is fairly straight forward, and usually initiated by the cleared firm, is provided in Figure 3.2. As described in Section E above, DoD security regulations (1991) provide the Form 441S "Certificate Pertaining to Foreign Interests" (Figure 2.4) as the primary avenue for reporting FOCI information. The reporting requirements section of the regulations, however, specify that in the case of a change in ownership, operating name, or when entering into discussions with foreign interests which may increase the level of FOCI, the firm must report the details to the Defense Investigative Service by letter. Such reports, when submitted in confidence, are protected from unauthorized disclosure under the applicable exemptions of the Freedom of Information Act. The DIS and the cleared firm work together to develop a case file

- No
Se
44
For
me

- Ga
cla
tat
(RR

- Neg
cour
able
using

- Votin
- Prox
- Boar
- Spec
- Recip

- Imple
- Notify
- Report

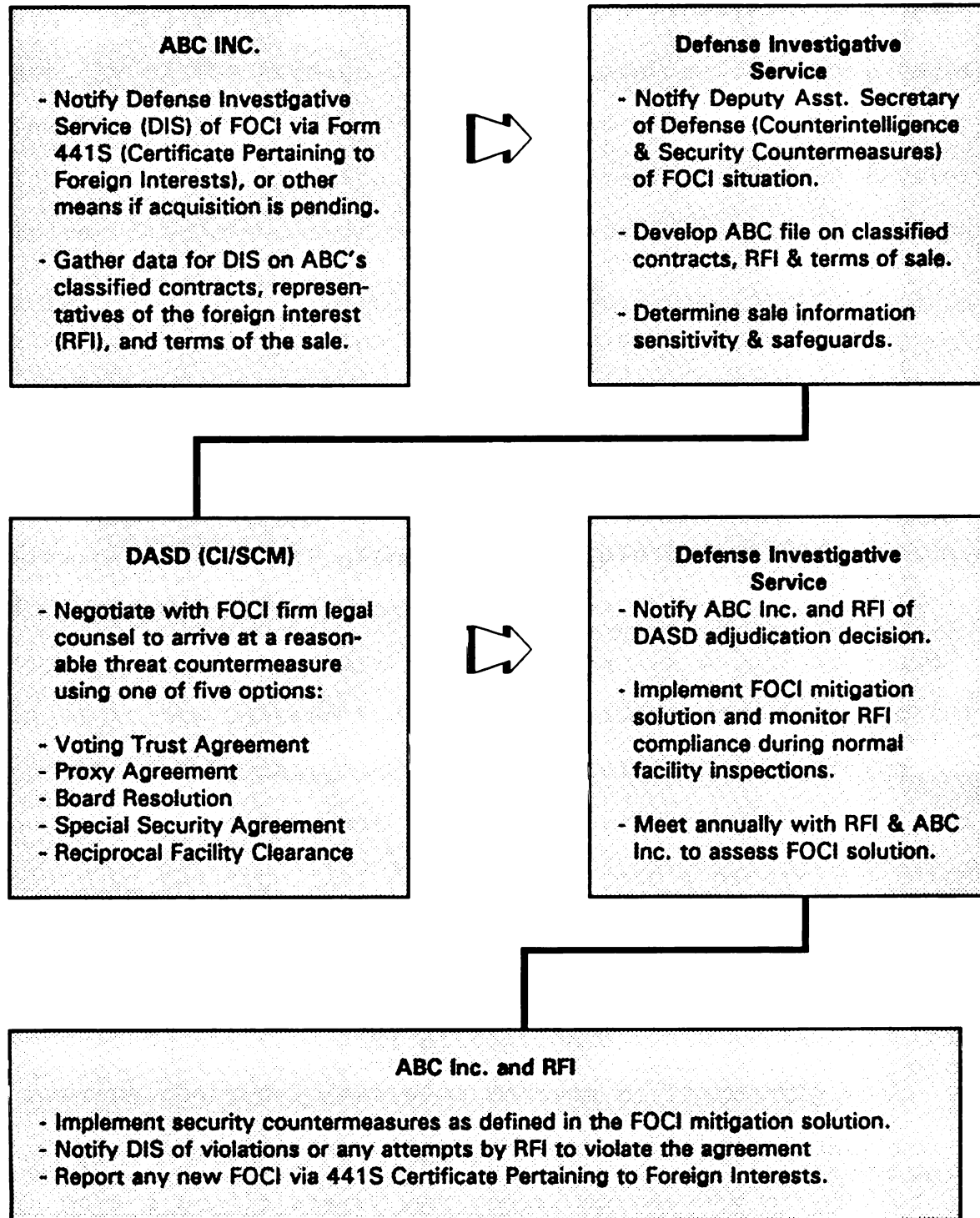


Figure 3.2

DISP FOCI Adjudication Process Model

cont

det:

the

app

in :

step

dec

Secr

Coun

firm

in p

appro

negot

spear

compa

hired

relat

or bus

sugges

three

to two

Terms a

dependi

depth of

concern

manifeste

containing a description of the firm's classified contracts, details of the foreign direct investment and, if applicable, the terms of the sale. The firm must also comply with other applicable federal reporting requirements described earlier in Section D.

Depending on the complexities of the case, the second step of the process involves notification of the policy decision-makers in the office of the Deputy Assistant Secretary of Defense (Counterintelligence and Security Countermeasures). These officials complete the cleared firm's case file by gathering available threat information in preparation for process step three, negotiation of an appropriate FOCI security countermeasures solution. Such negotiations between the firm and the government may be spearheaded by management of the acquired and acquiring companies, but frequently involve specialized legal counsel hired by the acquiring firm to negotiate a parent/subsidiary relationship that is conducive with its operating philosophy or business objectives as the parent. As previously suggested, the five FOCI mitigation options listed in block three of the model (see also Section E) frequently boil down to two, a Special Security Agreement or Voting Trust/Proxy. Terms and conditions of individual agreements may differ depending on the preferences of the foreign investor, the depth of security at the cleared firm, and the level of concern in the Department of Defense about the FOCI threat manifested in the case.

who

Def

inv

mak

the

sec

fiv

not.

secu

cert

work

comm

effi

thre

the

view

seve

the

Posi

1.

since

foreign

Likewis

foreign

Case adjudication may, or may not, require use of the whole model. Less serious FOCI threats may be mitigated by Defense Investigative Service field personnel without the involvement of DIS headquarters staff, or Pentagon policy-makers. Once an agreement is finalized, the fourth step of the process is invoked where the firm implements the security provisions, and the DIS monitors compliance. Step five recycles the process if FOCI again increases, or DIS notification is required due to an act of non-compliance.

The following critical examination of DISP FOCI security regulations suggests that the process is marked by certain attributes that work, and others which need some work. First, two observations about the current process commend it from a macro perspective, specifically its efficacy as relates to other broad U.S. policy goals. Then, three additional observations point out technical aspects of the process which work well from a security countermeasures viewpoint. These discussions are followed by analysis of several technical shortcomings which form the gap between the Voice of the Customer and the Voice of the Process.

Positive Notes - What Works

1. Consistency with Foreign Investment Policy

There are numerous economic and political reasons why, since World War II, the U.S. has predominantly encouraged foreign direct investment (Hanson, 1989, Section C above). Likewise, there is a nearly equal number of reasons why foreigners have taken advantage of available investment

op

for

due

For

ing

pol

inv

tre

same

proc

cons

inves

Secre

curre

inves

been

contin

the ba

grappl

presen

operati

Evidenc

adjudica

policy o

"Interim

from Pag

opportunities. It would be difficult to definitively forecast what policy future Administrations will endorse, or due to political or economic pressures, be forced to adopt. For the time being, as Hanson indicates, there are key ingredients of the current "open door" foreign investment policy: 1) the U.S. approach offers no special incentives to investors; 2) it imposes no special barriers; and 3) it treats established foreign-owned firms substantially the same as domestic companies (1989).

One of the positive aspects of the FOCI adjudication process of the DISP is that, over the years, it has been consistent with Hanson's three observations about foreign investment policy. Officials from the Office of the Secretary of Defense told the GAO (1990, March 21) that current DoD policy neither encourages or discourages foreign investment. Numerous policy and procedural adjustments have been phased in over the years, and security practices are continuously evaluated as new information is received, but the basic principle is unchanged. As defense policymakers grapple with increasing threats to technology, such as those present in the Thomson CSF deal, maintaining the basic operating philosophy will become increasingly difficult. Evidence of a tendency to use the industrial security FOCI adjudication process as a vehicle to impose protectionist policy objectives appeared in the Stewart (1992, August 28) "Interim guidance for FOCI cases." The following paragraph from Pagliano's (1992) report to Congress on foreign

inv

suc

2.

DoD i

highl

proces

Field

compan

to bene

essenti

exclusi

the nati

ability

investment in U.S. defense companies however, cautions that such tendencies could produce grave consequences:

As McDonnell Douglas and other U.S. contractors experience the turbulence of coping with new market realities, foreign investment issues will continue to be a major focus of attention. Certain caveats apply to the current situation, and need to be weighed by U.S. policymakers. Demanding or making public too much information or putting too many restrictions on foreign investment could be detrimental to U.S. companies and the U.S. economy. Such actions could discourage foreign investment in the United States, and lead to retaliation against U.S. overseas investment. They could also disrupt alliance relations as the U.S. and its allies seek to cope with the impact of shrinking defense industrial bases. Cost-sharing among allied governments will be increasingly attractive as their defense budgets continue to decline in the foreseeable future. Also, cost-sharing among U.S. and foreign companies in non-defense and dual-use sectors will undoubtedly increase. The boundaries of strategic technologies are continuously changing as new technological advances take place. Defining those boundaries, and making sure that the best interests of the United States are served in an era of increasing foreign dependency will be a major challenge to U.S. policymakers.

2. Defense Technology Access

In expressing his views on DoD's FOCI review process, DoD industrial security policy official John Frields (1988), highlighted the fact that the DoD foreign investment review process has evolved responsibly over more than thirty years. Frields stated that the DoD supports clearing foreign-owned companies, consistent with its policy, since the U.S. stands to benefit by having available products or technologies essential to the defense mission that cannot be attained exclusively from U.S.-owned enterprises. A determination of the national interest, and a confirmation of the firm's ability to protect classified information, guide decisions

to re

crea

coun

Frie

indu

tech

durin

divi

Foree

inves

natio

to th

cited

devel

II, t

under

effor

the w

techno

Conseq

design

develop

Th

steadily

developm

amounts

to release sensitive information to foreign-owned firms.

Complex cases such as Thomson CSF will necessitate creativity and flexibility in NISP FOCI policy and security countermeasures development. Nevertheless, support for Frields' opinion on the criticality of a viable defense industrial base and the need for access to leading-edge technology, whether U.S. or foreign-owned, was demonstrated during Thomson's unsuccessful bid to acquire the LTV missile division. Thomson contracted Washington-based Defense Forecasts, Inc., to prepare a paper (1992) titled, "Foreign investment in the U.S. defense industrial base: A sound national strategy for America's future." Obviously slanted to the French investor's interests, the paper nevertheless cited official DoD views on the value of foreign-owned or developed technology. It suggested that following World War II, the U.S. stood as the only Western nation capable of undertaking large-scale military research and development efforts. As Europe labored to overcome the destruction of the war, U.S. defense planners invested heavily in defense technology to counter the threat posed by the Soviet Union. Consequently, for much of the post-war period, U.S. weapon designers and manufacturers were relatively free to ignore developments overseas.

This is no longer the case. Defense Forecasts cited steadily increasing European nation military research and development spending figures over the past 20 years. The amounts are small in comparison to U.S. expenditures over

the
sign
proc
requ
whic
affe
cent
broa
"imp
rese
indic
have
paper
allie
techn
3.

sugge
izpac
struc
hiera
many
(e.g.
Taylo
the r
(Cunn.
manage

the same period, but did give America's European allies significant capabilities in key technological areas. As proof, the paper referenced a DoD report, generated at the request of Congress (1991, and 1990 version, Footnote 1), which identified 21 broad technological areas which will affect the nature of warfare for over the next quarter century. Part of the DoD's report, listed 10 of the 21 broad fields where America's European allies could make "important" or "substantial" contributions to U.S. defense research and development efforts. In fact, the DoD indicated that in many areas, European and Japanese firms have matched or surpassed American advancements. In its paper, Defense Forecasts suggested that in many cases, allied efforts complement, rather than compete with, U.S. technological capabilities.

3. Defense Security Committee (DSC)

Two recognized axioms of the security profession suggest that the effectiveness of the function is directly impacted by its placement in the corporate organizational structure, and the degree of support it receives from the hierarchial apex of that structure. This theme surfaces in many security management text discussions on organization (e.g., Green, 1981; Healy & Walsh, 1971; Cunningham & Taylor, 1985; Timm & Christian, 1991). Seventy percent of the respondents to a 1981 Security World survey (Cunningham & Taylor, 1985) indicated that their security manager reported to the company's chairperson, chief

executive officer, president, vice president of operations or finance, or general manager. Serving a staff function, the modern security professional is an advisor to senior management. Despite this trend, they are not being given carte blanche to accomplish their mission. Consequently, the security manager must be able to show how sound security measures enhance and contribute to business objectives, or else the resources necessary for adequate security may be limited (Criscuoli, 1988). Demonstration of the return on investment associated with a security policy, procedure, or other initiative, can result in an influential ally in the chief executive officer.

The NISP illustrates the importance of this alliance. The clout of AIA chief executives, who recognized a huge cost savings potential, facilitated NISP presentations to senior government officials. On their own, AIA security managers probably would not have been able to meet with agency directors and members of the President's cabinet. Once these government executives heard the NISP message, resource woes impacting their organizations caused them to grasp the concept's value and reject lower-level resistance to it. Their collective endorsement convinced the National Security Advisor and the President to support it.

Further testimony on the importance of senior management support of security came in the wake of the 1985 Walker spy ring discovery. To reduce the potential for further acts of espionage, Defense Secretary Weinburger

estab

recon

Comm

acce

The C

role

respo

a sta

manag

servi

FOCI

Comm

a maj

Typic

truste

affili

Proxies

citizen

who have

allegian

The DSC,

established a DoD Security Review Commission which made 63 recommendations for policy and procedure enhancement. The Commission's report included the following statement which accentuates the senior management support issue:

Security is everybody's business and, most notably, that of the individual in charge. As with all other responsibilities vested in them, it is incumbent upon commanders and supervisors to underscore the importance of the security function by personal example, by setting forth the rules, by inspecting for compliance, and by disciplining those who fall short (DOD Security Review Commission, 1985).

The Commission's comments suggest an active participatory role by senior management, rather than simple delegation of responsibility to the security office. Placing security in a staff position is not sufficient for comprehensive risk management, especially if company officials only pay lip-service to security goals and objectives.

To ensure proactive management support for security in FOCI companies, the DoD created the Defense Security Committee (DSC) concept. DoD FOCI arrangements require that a majority of the corporate board members be U.S. citizens. Typically, such boards will include a number of proxies, trustees, or "outside" directors who have had no former affiliation with the U.S. company or the foreign parent. Proxies, trustees, or outside directors are often prominent citizens, such as retired military officers of flag rank, who have previously held a security clearance and whose allegiance to the U.S. government is a matter of record. The DSC, as a FOCI security countermeasure, is a permanent

commi

proce

secur

cons:

secur

direc

secre

"wat

post:

from

Disc

matt

by tl

repr

meet

the

impl

chro

pert:

fore:

DSC n

with

ackno

respon

ensure

Th

securit

committee of the corporate board responsible for all procedures, organizational matters, and other aspects of security and technology export-control management. The DSC consists of the U.S. citizen board members and the firm's security manager who is a non-voting member. One of the directors is designated as DSC chairman, another as DSC secretary. DSC members fulfill a role as government "watchdogs" and enhance the foreign-owned firm's security posture by insulating or isolating the subsidiary executives from adverse management control exercised by the parent. Discussions of classified and export-controlled technical matters by the DSC are held in closed sessions, not attended by the foreign nationals who are only allowed minority representation on the corporate board. Minutes of DSC meetings, and all other pertinent records, are presented to the DoD as part of an annual report on FOCI arrangement implementation. The DSC report also generally includes a chronology of significant events, a description of matters pertaining to compliance or noncompliance, and a record of foreign parent visits to the U.S. firm approved by the DSC. DSC members hold personnel security clearances commensurate with the level of the firm's facility clearance. They acknowledge annually, by written certification, the responsibility the U.S. government has vested in them to ensure compliance with the FOCI security arrangement.

The DSC may be the key to revolutionary enhancement of security management in all cleared firms, U.S. or

foreign-owned, because it forces senior staff to enter into an active partnership with the security office. The security manager becomes a technical staff advisor to the DSC, and action officer for most of its initiatives. The security manager and the DSC, or at least its chairperson, interface routinely on important security issues and usually meet quarterly. The security manager formulates security policy and procedures that are promulgated under the auspices of the DSC which improves organizational adherence.

The boost in authority for the security manager comes at a price, highly scrutinized accountability. Security directors have complained for years that it is difficult to shed the "corporate cop" image and gain respect as a valued business executive. For the security manager involved with a DSC, getting management's attention is not a problem. Regular interface with corporate directors allows ample opportunity to prove management skill. FOCI arrangements require an annual review meeting with the DoD, generally held in conjunction with a meeting of the board of directors which is the report card for the security program. Thrust into the limelight before the corporate board and DoD auditors, the security manager either showcases a sound security posture, or else. Corporate directors do not like to be embarrassed and usually will not tolerate unprofessional mediocrity by the security manager.

Another benefit of the DSC concept is that it allows the security manager to demonstrate the requirements of the

fu

st

ol

se

as

me

wl

tl

be

fo

se

st

wl

ol

co

se

in

da

DS

in

in

pr

in

se

ex

ins

Dir

function. Often, security is misinterpreted in one of two stereotypical ways, as a department shrouded in the secrets of classified material, or as the "guards." In either case, security is often not taken seriously because it is viewed as a revenue drain. Frustration is common for security managers reporting to human resources or finance managers who neither understand or desire to learn the job, and therefore delegate all responsibility. This style can be beneficial, or catastrophic if security's budget is not forthcoming because a request is not understood.

One final benefit of the DSC is that it gives the security manager recognized authority in the organization when conducting sensitive internal investigations. Obstructions may surface in cases involving violation of company or government policy such as fraud, waste, or abuse. Senior staff, even if not implicated, may stonewall an inquiry if it appears the allegations could result in damaging evidence of unsatisfactory managerial performance. DSC backing allows security to overcome such hurdles.

The DoD confirmed the value of senior staff involvement in security in 1987 by implementing "Project Insight." The project instituted several industrial security inspection improvements, including one expressly created to increase senior management participation. Specifically, chief executive entrance and exit briefings were added to security inspections. Such inspections, by regulation, (DoD Directives 5220.22-R & 5220.22-M) are normally done

se

or

ma

pr

ma

re

se

th

4.

cr

Do

of

co

Sp

cl

in

go

co

ma

em

en

act

esp

int

ensi

DSC.

semi-annually and range from one day to two weeks, with one or more inspectors. The Insight briefings provide senior management the government's view of the firm's security program. Inspections are taken seriously by senior management because an unsatisfactory rating can result in revocation of the facility clearance. Revocation can severely damage or bankrupt a company that is dependent on the government for most of its business.

4. Security Awareness

Employee security awareness, training and education are critical to the effectiveness of any security program. Dr. Donald Hicks (1990) makes the assertion that secrecy is officially protected just as rigorously with foreign-owned contractors as with the American ones. He suggests, the Special Security Agreement arrangement probably makes classified information better protected in contracts involving foreign firms. This may be true since some government officials are skeptical about the SSA, therefore compliance with the agreement is viewed by employees and management as critical to business survival. Additionally, employee security awareness in an SSA cleared firm is enhanced when DSC members lead by example and are observed actively participating in the program. The benefits are especially apparent when DSC directors follow up on foreign interest visits by contacting the U.S. employee host to ensure discussions stayed within the scope approved by the DSC. Employees naturally spread the word about contacts by

6

2

f

p

5

co

m

A

T

c

c

pr

unc

categ

global

Directors which proves to their co-workers that management is serious about security. The same security awareness impact is not realized when the contact originates from the security manager because he is perceived as a peer or subordinate, rather than a superior. Such DSC contacts directly apply the DoD Security Review Commission's point about the commander leading by personal example, by setting forth the rules, by auditing for compliance, and by punishing noncompliance.

5. Export Control Compliance

Traditionally, the DISP has placed little emphasis on compliance with the Arms Export Control Act (1976) for military goods (except classified items), and the Export Administration Act (1985) for commercial and dual-use goods. The Arms Export Control Act covers the export of defense articles and related technologies to foreign persons, and is the basis for the International Traffic in Arms Regulation (1987) administered by the State Department Office of Defense Trade Controls. The Export Administration Act is the basis for the Export Administration Regulation (1987) which the Bureau of Export Administration is responsible for in the Department of Commerce. Given the limited oversight capabilities of State and Commerce, the feasibility and prudence of expanding the scope of DISP oversight to these unclassified but sensitive export-controlled classification categories has been debated. As the NISP evolves and the global market shrinks, the debate becomes more intense.

While not designed as such, a pilot program for enhancing contractor compliance with export-control regulations currently exists in the implementing arrangements of DISP FOCI security policy. The threat of unauthorized technology transfer inherent in FOCI situations caused the DoD to incorporate export-control compliance provisions into the language of Voting Trust, Proxy, and Special Security Agreements. The result has been an overall improvement in the security posture of FOCI firms where export-control issues become an integral part of daily operations. The rules regarding disclosure of classified material to a foreign parent are quite clear. Conversely, compliance with export control regulations, where the rules often require interpretation, takes more effort. Hence, the cleared contractor under FOCI must appoint an Export Control Officer (ECO) to monitor transactions with the foreign interest or parent company. Frequently, technical exchanges necessitate an export license from the Department of State or Commerce, and development of a Technology Control Plan (TCP). The TCP prescribes all security measures necessary to foreclose the possibility of inadvertent access by non-U.S. citizen employees and visitors to information for which an export license is required. Unique badges, escort procedures, segregated work areas, security indoctrination schemes, and other measures may be included as appropriate. The TCP also provides a method to ensure information exchanges with the foreign interest are reviewed and

C
C
A
C
C
W
C
S
th
Se
re
ac
sh
ost
ste
Tiar

approved in advance by the security manager or the ECO. The ECO gives advice to management, employees traveling internationally, and to persons hosting foreign customers or parent company visitors. The improvements in FOCI firm export control compliance observed by DIS provide a compelling argument that the practices should be incorporated into the security programs of U.S.-owned firms as well.

Negative Notes - What Needs Work

6. FOCI National Security Intelligence, Threat Assessment and Risk Analysis

Foreign direct investment in U.S. industry receives Congressional scrutiny through the review processes described in Section D above. Additionally, the Exon-Florio Amendment provides Presidential review authority through the CFIUS process which requires a swift and structured review of national security significant foreign direct investment. Wartzman (1992, November 2) points out, however, that critics have long complained that CFIUS is just a rubber stamp. Of more than 700 deals it formally examined before the Thomson case, it gave all but 13 just a cursory review. Several companies, like Thomson, walked away after sensing rejection. The panel reversed only one transaction, a 1989 acquisition of Mamco Manufacturing Inc., a Seattle machine shop that makes aircraft parts, by the Chinese. The ostensible reason was that the Chinese had once tried to steal U.S. jet-engine technology, though outrage over Tiananmen Square may have been as much of a motive.

In the aftermath of the Thomson case, Congress generated legislation, which the President signed, that underscored the fact that the wisdom of policy decisions regarding the national security ramifications of individual FOCI cases is dependent upon the quality and timeliness of intelligence assessments it receives from the Executive branch, in particular the Department of Defense. Specifically, the Defense Authorization Conference for fiscal 1993 legislated "Improved National Defense Control of Technology Diversions Overseas" (1992) which required:

- a database be established from 1988 forward on all contracts over \$100,000 awarded to FOCI entities;
- an annual report to Congress analyzing those contract awards covering defense critical technologies;
- in any pending or proposed merger, acquisition or takeover of a U.S. company doing work in a defense critical technology area by a FOCI entity, the Secretary of Defense shall have a risk assessment conducted by the Defense Intelligence Agency, the Army Foreign Technology Science Center, the Naval Maritime Intelligence Center, and the Air Force Foreign Aerospace Science and Technology Center.

The first two Congressional requirements are fairly straight forward. Information on contracts awarded over \$100,000 is readily available from the various procuring activities of the Executive Branch. Analysis of defense critical technology contracts awarded to FOCI firms can be

accomplished by a number of government agencies. The requirement for the Secretary of Defense to conduct FOCI risk assessments is however, a little more difficult because it presupposes that intelligence information is available.

A critical look at the Secretary of Defense's requirement to have FOCI risk assessments conducted requires some understanding of intelligence operations. Carter's (1990) model of the intelligence gathering process provides a framework to organize a critique of DoD capabilities. Carter describes intelligence operations as a sequential process which includes: collection of raw data; evaluation of information reliability and validity; integration and analysis of information; and, dissemination of a final product to authorized consumers. These same steps are traced in the following review of the efficiency and effectiveness of DoD FOCI intelligence operations.

a. Collection

In 1991, the NISP FOCI Working Group (Frields, Muscat, 1991, April 16) requested a threat assessment on foreign direct investment in U.S. high-technology from the NISP Threat Working Group. The assessment was to be used by the FOCI Working Group to develop threat driven security countermeasures. Additionally, the NISP Oversight and Compliance Working Group would use the assessment to develop criteria for use by the industrial security inspection cadre under the NISP. The parameters set forth to the Threat Working Group included specific interest in situations where

the investor exercises partial or total control over a firm, normally through ownership, directly or indirectly, by a person or firm of 10 percent or more of the voting securities of the corporation. Cases with ownership of 50 percent or more of the voting stock by a foreign interest were highlighted as being of greatest concern.

Due to the accelerated schedule of the NISP, the Threat Working Group (Brandon, 1991, May 30) declined to accomplish an industry specific foreign direct investment threat assessment. Recognizing foreign direct investment as an important element of the larger national security intelligence picture, the Threat Working Group referred to its stated objective of preparing a "Catalogue of Threat Assessments" designed to provide a broad-based assessment relevant to the NISP and the future needs of U.S. industry. The Threat Working Group pointed out that only a limited body of knowledge on FOCI exists within the Defense Intelligence Agency (DIA), Defense Technologies Resources Group DIA/DT-5B. Since the DIA personnel consulted by the Threat Working Group were already members of the FOCI Working Group, efforts to develop countermeasures continued without an updated threat assessment.

The lack of FOCI intelligence information makes it difficult to quantify threat and develop appropriate security countermeasures. Department of Defense industrial security regulations (DoD ISM 520.22-M, 1991) require contractors cleared to work on classified defense contracts

Y
r
q
e
t
r
"r
ur
Co

to prepare a Certificate Pertaining to Foreign Interests, DD Form 441S (see Section E, Figure 2.4). While the Form 441S filing is required as part of the DD Form 441 Security Agreement (DoD ISM 5220.22-M, 1991, and see Section E, Figure 2.3) that industry executes with the government, it nevertheless can be viewed as a voluntary intelligence collection method producing questionable results. Failure by the contractor to answer all questions, or any intentional misrepresentation, may serve as a basis for denial of clearance for access to classified defense information or grounds for prosecution under Title 18, U.S. Code 1001, which is highlighted in the Penalty Notice of the Form 441S. Nevertheless, the voluntary nature of the information gathering process suggests a less than objective product, perhaps as accurate as the cumulative summary of federal income taxes reported by Americans each year.

b. Evaluation of Reliability and Validity

Despite the penalty clause, the reliability and validity of information supplied by industry on Form 441S responses is also suspect due to the ambiguity of the questions. Industry security professionals have long expressed frustration to DoD officials about their attempts to obtain accurate contract and finance information requested on the Form 441S. For example, Question 5 asks, "Does your organization have any contracts, agreements, understandings or arrangements with a foreign interest(s)?" Confusion exists about whether this question refers only to

major contracts, or if it is intended to include large subcontracts and small parts purchases such as Japanese electronics components. Depending on who fills out the form, responses may vary radically without malicious intent to deceive the government. Responding to this problem, the FOCI Working Group pledged to the NISP Steering Committee in its goals and objectives (1991) that it would ensure more consistent and accurate responses to the survey by creating a new form, complete with a set of clarifying instructions.

Reliability and validity of information supplied on the Form 441S is also questionable from another perspective. It is, for instance, unlikely that a contractor applying for a capital improvement loan or research and development funding would realize, or be able to determine, that the lending institution is controlled by a foreign entity. A random sample audit of Form 441S filings of both large or small firms might therefore reveal a surprising, perhaps shocking picture of the real extent of FOCI in the defense industry.

Additionally, the thresholds of tolerance on the Form 441S raise other reliability and validity issues. In three questions, a 5 or 10 percent level of income, ownership of securities, or nominee shares is identified as establishing a FOCI situation at the firm. In the rapidly expanding global marketplace, the probability that a U.S. firm with a number of foreign customers could be considered under FOCI, yet still fall well short of a majority percentage of foreign ownership, is fairly high. Further, the customer

1
C
C

R
g
s
p

Ex
se
Se

Ag
Adv
inc
and

cont
inte
exis
Fore.

base of most firms is dynamic, changing daily in many cases. It would therefore be possible for a firm to routinely fluctuate in and out of FOCI parameters, certainly more rapidly than the 441S could be updated and adjudicated.

One final concern arises regarding the significance of the seemingly arbitrary 5 and 10 percent FOCI thresholds established on the Form 441S. It raises the question, is 11 percent FOCI income, stock ownership, or nominee share control more alarming than 10 percent? If so, why?

c. Integration & Analysis

The Defense Intelligence Agency, Defense Technologies Resources Group (Swim, 1991) has developed a FOCI intelligence automated information system. The purpose of the system is to develop a series of relational databases to provide an integrated core of key information for analysis. Examples of existing databases included in the relational series are those available from: the Defense Technical Services Administration; the Federal Emergency Management Agency; the Defense Logistics Agency; and the Defense Advanced Research Projects Agency. Other examples may include financial data from commercial sources such as Dunn and Bradstreet.

Swim indicates that it is difficult in defense contracts to determine corporate ownership since a specific intelligence database on acquisition does not currently exist. Such information suggests that the Committee on Foreign Investment in the U.S. (CFIUS) currently has

insufficient data for informed Exon-Florio determinations. Of particular interest to DIA are the foreign "spoilers" whose motivation is to pilfer U.S. high-technology from small firms, then sell or close them. Swim suggests that with its new database, DIA will initially look at the "high poles in the tent" for proliferation considerations and technology pilferage. He defines the high poles as foreign investors who come back every year to buy more and more U.S. technology, clearly a national security concern.

In 1991, Swim indicated that DIA faced an uphill battle in its efforts to establish a FOCI database. At that time the biggest challenge was to convince the policymakers that intelligence priorities were changing from those which dominated the traditional militarily-oriented standoff, to those of the new economic war. While attempting to define its new role in the post cold-war era, the Intelligence Community³ struggled to recognize that foreign acquisition of the defense industrial base was becoming one of the more important threats of the future. In 1992, however, the Thomson case crystallized the reality of changing times, and the Defense Authorization Conference for fiscal year 1993 legislated some new intelligence gathering priorities.

The effectiveness of the DIA database venture will, in part, depend upon the ability of agencies with what Carter (1990) defines as "exclusive" intelligence gathering responsibilities focused only on national policy missions (like those of the Central Intelligence Agency, Defense

Intelligence Agency, National Security Agency) to cooperate amongst themselves, and with those agencies who have "non-exclusive" responsibilities (national policy and law enforcement like the Federal Bureau of Investigation, Drug Enforcement Agency, and U.S. Customs Service). In the cold-war world when the threat (Soviet Communism) was clearly understood, the spheres of responsibility of the various intelligence agencies became institutionalized. Now, in an era of regional conflicts and rapidly changing intelligence interests, a process modification may be required. The traditional split of intelligence responsibilities along foreign (CIA) versus domestic (FBI) lines may no longer be successful. For example, an accurate domestic intelligence picture of the U.S. operations of a foreign-owned firm, and its ability to protect sensitive and classified technology, has significant importance. However, if considered from a non-proliferation viewpoint (especially nuclear, biological, and chemical weapons of mass destruction), intelligence on the foreign parent or government may have equal or greater value. This concept of a complex, comprehensive FOCI intelligence product describing the threat posed by an entire corporate lineage, suggests an integrated foreign and domestic intelligence apparatus which may require a cultural adjustment to achieve the necessary level of coordination amongst competing federal intelligence resources. Anything less would result in an incomplete FOCI risk assessment, and insufficient security countermeasures.

Finally, there is a notable difference in the FOCI analysis and adjudication methodology employed by the various federal agencies who contract with FOCI firms. In determining whether to grant or continue a firm's clearance for access to classified information when FOCI occurs, the Departments of Defense and Energy differ from the Central Intelligence Agency. The CIA assembles experts with intelligence, security, legal, and acquisition backgrounds. Defense (which also reviews FOCI cases on behalf of 20 non-Defense agencies) and Energy generally use only security and legal experts. Defense occasionally uses acquisition personnel when conditions warrant. The CIA review seems to be more comprehensive, and perhaps more effective.

d. Dissemination

Since the Form 441S requests information that describes the competitive business posture of the firm, an issue of consequence to industry is the privacy considerations. The Defense Investigative Service, which is chartered to review the forms pursuant to the granting and continuance of a facility clearance, will ensure confidential handling of the data, if requested. Frequently however, government customers, especially in the procurement branch of the military components request a copy of the form when awarding a contract. Contractors, worry that the same level of care is not afforded the documentation in these other organizations. Unfairly disclosed competitive sensitive information could be devastating, especially to smaller firms.

A related issue of competitive sensitivity surrounds the access controls established for the DIA FOCI database. Given the previously addressed Form 441S privacy issues, the automation of such data, compounded by a diverse and distributed network of users, gives cause for alarm. Many concerns arise from the business perspective: identification of the user community; confidence in the system's software access controls designed to prevent data manipulation; and safeguards for data integrity to ensure accurate information supplied by the contractor is not altered. Given access to competitive sensitive information, such as the financial well-being of a company or its merger and acquisition history, unethical firms could develop a strategy to sabotage corporate growth objectives of their competition. Inaccurate data viewed by a procurement official that results in the elimination of a viable competitor for a defense contract is not in the best interests of the government or the firm. The frequency of dissemination for strategic and tactical intelligence purposes may also be of consequence. Since the database is primarily for national security risk assessment purposes, procurement branches of the defense agencies should perhaps not be on distribution. That way, appropriately cleared FOCI firms are less likely to be eliminated from competition due to unjustified protectionist viewpoints about foreign direct investment. These DIA database information dissemination issues affect both foreign-owned and U.S.-owned firms.

7. National Interest Determination (NID)

As described in Section E above, when a foreign interest acquires a majority of the voting stock of a cleared U.S. firm, or effectively controls its management or operations and refuses to relinquish that control, DoD regulations (1991) allow a facility security clearance to be granted under the terms of a Special Security Agreement, or SSA. The SSA allows a majority foreign investor to have minority representation on the Board of Directors of the cleared U.S. firm. The SSA allows flexibility in the design of security countermeasures which are tailored to the risk, nature, and extent of FOCI in the case. A Reciprocal Security Agreement must be in place with the nation from which the FOCI stems, and only U.S. citizens are allowed access to classified material in connection with the facility security clearance.

A SSA is generally granted at the SECRET level or lower after a National Interest Determination (NID) has been accomplished by DoD security officials and the procuring military component or government agency. Information packets presented to contractors pursuing a SSA by the Office of the Secretary of Defense indicate that, as a general rule, a favorable NID includes:

an essential, impending, or prospective need to use, on a classified basis, the products, services, or technical expertise of a U.S. firm under FOCI when cleared or clearable firms are unavailable or insufficient to satisfy industrial preparedness, mobilization, planning research, production, or production base requirements of a Department of Defense component or a participating non-DoD agency.⁴

The NID is processed through the procurement channels of the government agency(s) or military component(s) that have contracted with the firm that has come under FOCI. Starting with the government Contracting Officer, the NID moves up the chain of command in the military service or agency and over to the Industrial Security function in the Office of the Secretary of Defense. In parallel, the contractor is usually providing the procurement officials justification to support the requirements of the NID. While the NID is processed, the contractor's facility security clearance is usually invalidated, which means it cannot receive new classified contracts. Given interim security measures, it may continue performance on existing programs.

Generally, SSA cleared companies are not allowed access to the highly sensitive "proscribed" categories of classified information listed below. If the company has proscribed contracts when acquired, the NID process can take up to two years, while the government considers novation or assignment of the sensitive contracts. Meanwhile the firm's facility clearance remains invalid, a devastating setback to new business growth. Proscribed categories include:

- TOP SECRET information
- Communications Security (COMSEC) information
- Restricted Data, as defined in the U.S. Atomic Energy Act of 1954, as amended
- Special Access Program information
- Sensitive Compartmented Information

On occasion, based on an overriding need or sole source justification demonstrated during the NID process, a policy waiver is granted by an authorized government agency which allows the contractor access to proscribed classified material for contracts existing at the time of acquisition. Such waivers may also be granted at a later date for a specific government procurement.

The GAO (1990, March 21), however, found the NID process lacking. The GAO reported to Congress that the services' implementing policies and procedures for NIDs require procurement activities to justify a need for a product or service that is mission-critical, cannot be obtained in sufficient quantity from U.S.-owned sources, and involves a unique product or technology. Military service security officials interviewed by the GAO indicated that supporting justification for these determinations is sometimes incomplete or inadequate. The GAO also reported that in one SSA, several commands had requested the retention of almost every contract with the contractor without documenting the need in each case. In some cases, contracting officers did not indicate what steps, if any, were taken to identify U.S.-owned suppliers. In another case, the services' files indicated that several U.S. firms could fill the user's requirements, but an SSA was requested and approved. In another case, the foreign company requested approval of an SSA before it bought a U.S. firm. The SSA was approved by the takeover date.

The GAO findings demonstrated in 1990 that the NID process was not effective. The lack of supporting documentation for waiver decisions in the services' files may be attributable to the amount of effort required to compile such data. Realistically these files probably contribute little to procurement decisions because hesitancy over FOCI concerns tends to be overridden by the requirement to purchase the best available technology at the lowest possible price. Therefore, like an insurance policy, the files would only be useful in the event of a technology compromise, should it become necessary to prove to Congress that the procuring command satisfied all the regulatory steps. The GAO evidence shows the military components have opted, on occasion, not to pay the costly insurance premium because of its questionable value. Since the process has not changed since 1990, it is doubtful there has been any measurable improvement.

The GAO NID critique is unfortunately incomplete since it only describes the degree of compliance with the process as it is currently structured, not whether the process itself is effective. To properly critique the process, it is important to first step back and review the purpose of the NID from a security countermeasures perspective. Such reflection leads to the realization that the original intent is consistent with basic security principles and the national security imperative to identify the FOCI threat, quantify risks to classified material, and define security

countermeasures to protect such material in a manner acceptable to the government. For the reasons detailed below, however, in practical application the NID process does not achieve these important objectives.

Viewed as a security countermeasures process, the current NID appears misdirected. In its present format, the NID confirms military procurement needs as opposed to defining threat, risk, and security countermeasures. Specifically, the NID can be characterized as a process of "passing the buck" for acceptance of FOCI risk from the lowest ranked person in the procurement chain to, at minimum, an Assistant Secretary level in the procuring command. During the NID, each successive management level must assume FOCI risk responsibility so the foreign-owned technology source is maintained as a productive part of the defense industrial base. Oddly enough, the NID process does not include an effort to design security solutions to counter real or perceived threats to the sensitive or classified technology. The important and obvious, yet seemingly overlooked fact is that maintaining access to the best available technology in the defense industrial base, regardless of ownership, is clearly in the national security interest. Similarly, continuance of the American jobs in the contractor's facilities acquired by the foreign interest is in the national economic interest.

The real question, not properly addressed by the NID process is: given a defined FOCI threat and risk scenario,

what national security information safeguards would permit the firm to continue serving defense industrial base requirements? Acceptance of risk, using a very resource intense NID process that only reaffirms source selections and procurement needs without imposing threat driven security safeguards, is not productive for the government or industry, and is a waste of tax dollars.

Once a SSA is in place, the situation is exaggerated, and competition further stifled, as the NID process is repeated for new programs or other situations like classified meetings requiring access to proscribed information. New program NIDs normally cannot be processed in the forty-five to sixty days routinely allotted for the proposal stage of the procurement cycle. SSA cleared firms become especially exasperated when procurement officials put up roadblocks or initiate NID procedures for programs that do not contain proscribed category classified information, simply because they do not understand Department of Defense security policy.

To avoid losing out on major contract opportunities, SSA cleared contractors may resort to costly work-arounds like third-party contracts between the procuring activity and another U.S.-owned supplier of such expertise as TEMPEST evaluations (compromising electronic emanations) involving COMSEC material, or nuclear hardness (survivability) analysis involving Restricted Data. In these arrangements proscribed classified material is not provided to the SSA

firm. The third-party contractor reviews the SSA firm's design and delineates changes based on the requirements of the proscribed specification. Such arrangements work, but increase product development time and cost because the SSA cleared firm is essentially designing with one eye closed. Restricted Data and COMSEC facility clearance limitations more adversely impact the competitive posture of SSA firms than the other proscribed categories because of the prevalence of military specifications which include those types of material. Due to the limitations, procuring agencies are sometimes faced with losing a long-standing and valued supplier which adversely impacts the competitive nature of the procurement process.

In the final analysis, the GAO report seems to detail symptoms rather than the root cause of problems with the NID process. The interests of national security, the procuring government activity, and the FOCI firm would all be better served if the current system of risk "acceptance" were changed to a proactive process of risk "management." To accomplish that, a new approach to the issue of protecting proscribed information in FOCI firms is required.

8. Proscribed Information

There is no question that safeguarding proscribed information national security assets in cleared firms that come under FOCI should be the preeminent objective of the NID process. However, not all foreign investment poses the same level of threat, and not all countries are, or should

be treated equal. This premise is the heart of the "Special" Security Agreement concept where countermeasures are tailored to threat and risk. In some cases threat or risk may justify strict access limitations. In others, security solutions can negate FOCI risks, or reduce them to an acceptable level.

Unfortunately, as demonstrated in the Thomson CSF case, adjudication of FOCI cases can get politicized. Decisions may be biased by media influenced opinions of the business reputation of the foreign investor(s), or by the state of their country's relations with the U.S. at the time of investment. Political overtones can even overshadow the common sense evaluations of the value of the technology at stake and the consequences of its compromise. In order to downplay the political aspects of any given FOCI case, it is prudent to approach the NID from a sound national security policy foundation. That foundation already exists in the form of the U.S. National Disclosure Policy (NDP) and General Security of Information Agreements (GSOIA). Unfortunately, the U.S. government has not taken advantage of the rational NDP process to make "risk management" decisions as opposed to "politically correct" decisions.

The National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations (NDP-1, 1981) (Seymour, 1993) controls the release of classified U.S. defense articles and technology to foreign governments and is

promulgated in a classified directive. A NDP Committee, chaired by the Department of Defense and consisting of members from Defense, State, the Military departments, the Joint Staff, and other special members, is the controlling element for the U.S. Government's NDP program.

Disclosure authority and release considerations are based on legislation, national security policy, treaties, nonproliferation concerns, existence of General Security of Information Agreements (GSOIA), and other factors. The U.S. has negotiated GSOIA with several allied nations which facilitate the exchange of classified information between cooperating countries, and the safeguarding of such information in accordance with mutually acceptable standards.

The NDP Committee approves and maintains current Delegation Disclosure Letters (DDL) for each country, and forwards them to the Military Departments and other agencies for implementation and guidance. The DDL's specify levels of releasable classified information for each country, both in the general sense and specific to unique programs such as foreign military weapons sales.

When requests, either through Foreign Military Sales or an export license application, are received for a particular country, the Department of Defense will compare the request with the latest DDL for that country, and determine if the technology is authorized for release or if it would require an "exception to National Disclosure Policy." If an NDP exception is required, the case (or license application)

will be "returned without action," pending receipt of an "expression of interest" from the foreign country itself. Only a foreign country may submit such an expression, and only on a government-to-government basis, through its own Embassy in Washington, DC or through the U.S. Embassy in its country.

If an expression of interest is formally made by the foreign country, one of the members must agree to "sponsor" the exception to NDP, prepare supporting justification documentation, and staff it through the NDP exception review process. The sponsoring member must be convinced, through the justification submitted by the foreign government or the U.S. mission in that country, that an exception is in the national interest, is not precluded by law or treaty, and is desired by or considered beneficial to the Department of Defense and the sponsor. Sponsorship may also be initiated by an agency other than the Department of Defense, depending on the technology involved (e.g., nuclear matters, intelligence issues, space programs, etc).

The majority of NDP exception requests are approved. Most denials result from overriding foreign policy considerations, inhibiting legislation or national policy, lack of a GSOIA, conflicting treaty obligations, or insufficient justification. All NDP exception votes must be unanimous.

Foreign nationals investing in cleared U.S. firms possessing proscribed classified information likely will not

require, or if requested, be granted access to that material. However, if the GSOIA and disclosure policy for the country from which the FOCI stems otherwise allows for release of such material, then a reasonable basis exists for a favorable NID to authorize access to cleared U.S. citizens of the American subsidiary. The risks to proscribed information could be measured against two sets of criteria: (a) those used in developing the GSOIA and NDP for the nation(s) involved; and, (b) those adjudication criteria established authorizing cleared U.S. citizens access to such information when working for a U.S.-owned company. The degree of trust and responsibility placed on them, with or without foreign involvement, is after all the same. Finally, the decision would be fair because it would be traceable to bilateral agreements negotiated through diplomatic channels. If the foreign investor's government felt its company was being discriminated against, it could file an expression of interest on a government-to-government basis.

Given a sound policy foundation for proscribed information release to foreign-owned U.S. firms, the next step is to correct the shortcoming of the current NID by enhancing the security of such material in FOCI firms. A model for additional safeguards exists in the procedures already used for handling the material in U.S.-owned firms. Special Access and Sensitive Compartmented Information programs normally incorporate a number of supplemental controls including: special personnel background

investigations; a system to limit personnel access authorizations; special accountability procedures; and segregated storage with a higher degree of physical security protection. Building on this concept of supplemental protection, a carefully crafted and routinely audited set of security countermeasures designed specifically to safeguard proscribed information entrusted to FOCI firms would result in considerably more security than is presently derived from the NID system. More importantly, and consistent with the NISP goals and objectives, this enhanced level of security could be realized at less cost. For instance, if a set of security options were available to FOCI adjudicators, and the threat scenario warranted, they could be imposed immediately as the terms of the FOCI agreement are negotiated. If correctly implemented, the need to exercise the procurement arm of the services to justify equipment needs for an initial clearance or program specific access request would be eliminated. Countless manhours of government and industry time spent chasing risk acceptance signatures would be saved. Most importantly, the government will have efficiently imposed a much more effective security program to protect classified or sensitive technology.

9. Threat Emphasis and Security Countermeasure Development

Current FOCI security policy and associated countermeasures form a system that is only geared to deal with the tip of the threat iceberg. Approximately 100 high-profile majority ownership cases have received, by far, the most

attention from policymakers and the media. Meanwhile the threat posed by control or influence of the balance of the U.S.-owned defense industrial base seems to go unnoticed. Alliances, consortiums, licensing agreements, joint ventures, co-production programs, indebtedness to foreign lenders, and majority foreign supplier or customer dependency cases provide realistic examples of a much expanded FOCI picture. For instance, a small contractor deriving a large portion of its revenues from foreign customers without a set of isolation or insulation security controls like those in a Voting Trust, Proxy, SSA, or other arrangement, is perhaps at greater risk to compromising foreign influence than a properly cleared foreign-owned firm. A foreign interest seeking competitive business information, or cooperating in a state-sponsored intelligence operation, might be more successful at acquiring the technology it seeks by duping such a firm with a scam to purchase a single product, while it targets another technology. Such an approach would eliminate the need for a large capital investment to acquire the company, not to mention the government scrutiny and legal fees involved in obtaining a FOCI agreement.

Policymakers may have inadvertently developed an inaccurate picture of the real FOCI threat environment because of their preoccupation with a recognized set of security solutions. It may even be fair to suggest that marketplace globalization has rendered obsolete the U.S.

government's concept and operational definition of Foreign Ownership, Control, or Influence. FOCI is certainly not a security challenge that is unique to the U.S. government as evidenced by the extent of U.S. investment abroad. Instead, ownership, control, or influence of a world-wide network of corporate assets or trading partners is a key element of any multinational corporation's strategy to develop a global market presence. Some U.S. government officials are reluctant to acknowledge this trend, or the fact that U.S. industry no longer holds all the world's technological crown jewels, but rather a dwindling percentage. International economic competition will eventually force this realization, along with an understanding of the need for a threat driven, efficient, and effective menu of security countermeasures options to combat threats posed by all forms of foreign involvement, not just ownership.

The unhealthy dependence by policymakers on current FOCI security solutions is further highlighted by examining the focus and intent of such arrangements. In practical application, the Voting Trust, Proxy, and SSA differ somewhat; however, they all focus on control of the power and authority of corporate directors and senior managers. The idea that a compromise could occur because of adverse management impact or influence exercised by the parent or its representatives is valid, however, illicit classified or export-controlled technology transfer is more likely to occur at the engineer-to-engineer level. Professional

curiosity among U.S. and foreign colleagues, or eagerness to get the job done on joint ventures present more probable scenarios for inadvertent or intentional technology compromise. Current agreements provide considerable guidance on control of management data exchanges between the foreign parent and the cleared subsidiary, but little on controlling communication between the technology experts.

Therefore, to overcome the dependency on existing security solutions, with their inherent weaknesses, a paradigm shift is required. Such a shift could be initiated by eliminating the terms Board Resolution, Voting Trust, Proxy, SSA, and Reciprocal facility clearance. Deletion of the Reciprocal clearance concept is especially important because it does not incorporate the same type of legal contract between the foreign interest or the U.S. subsidiary and the U.S. government as the other arrangements. The limited effectiveness of these options, and the distinct aura that each has acquired, would be replaced by a simple, yet logical approach. Each cleared government contractor, regardless of the level of foreign ownership, control, or influence, would execute a NISP 441 Security Agreement with the entire Executive Branch of the government. Using the NDP and GSOIA as a foundation, as risk of classified technology increases due to greater foreign involvement, proportionate security countermeasures could be imposed as contract amendments to the NISP Form 441. In essence, the countermeasures imposed on the firm as technology protection

requirements above baseline standards in the NISP security regulations would correspond to real or perceived threats uncovered in the aforementioned improved National Interest Determination. The amendments to the NISP 441 might be similar to the terms of the current mechanisms; however, the handicaps to implementation caused by the mythical image that each has acquired would be eliminated. Further, depending on which Executive Branch department(s) or agency(s) used the products or services of the FOCI firm, amendments could be tailored to the unique requirements of that institution. CIA or DoE requirements might be more stringent than those of DoD to allow access to proscribed classified information. This approach incorporates the previously described methodology of factoring proscribed classified material supplemental controls into the strategy. Such a concept incorporates the basic NISP objective of threat driven, efficient, cost-effective security.

10. Security Agreement Violation Clauses

Under Executive Order 12356 (1982) National Security Information, the Information Security Oversight Office (ISOO, 1988) is responsible for monitoring the information security programs of all executive branch departments and agencies that create or handle national security information. In National Security Decision Directive No. 84, March 11, 1983, the President directed ISOO to develop and issue a standard "Classified Information Nondisclosure Agreement" (1988) to be executed by all cleared persons as a condition

of access to classified information. Threat of prosecution under applicable espionage and sabotage acts (18 U.S.C. §§ 793, 794, 798), other criminal and civil statutes and export control laws is an important deterrent in federal government efforts to safeguard classified information. Department of Defense security regulations (1991) require that persons cleared for access to classified information read the applicable federal statutes and acknowledge their responsibilities concerning unauthorized disclosure of classified information by executing a Standard Form (SF 312) "Classified Information Nondisclosure Agreement." The primary purpose of the SF 312 (ISOO, 1988) is to inform employees of (a) the trust that is placed in them by providing them access to classified information; (b) their responsibilities to protect that information from unauthorized disclosure; and (c) the consequences that may result from their failure to meet those responsibilities. Secondly, by establishing the nature of that trust, those responsibilities, and those consequences in the context of a contractual agreement, if that trust is violated, the U.S. will be in a better position to prevent an unauthorized disclosure or to discipline an employee responsible for such a disclosure by initiating a civil or administrative action.

Despite the carefully orchestrated legal boundaries placed around U.S. citizens as a condition for access to national secrets, interestingly enough, the same violation clauses are not detailed in security agreements established

with FOCI firms. Recognizing the obvious increase in risk associated with foreign involvement, rather than capitalize on the deterrent factor of espionage statutes by citing them as a consequence of noncompliance, facility clearance revocation is the most severe penalty established. Given the value of the information involved, and the views of protectionist critics who would opt for an isolationist policy, loss of clearance does not appear to be a big enough penalty to ensure adherence with the terms of the agreement.

For example, a hostile intelligence service or corrupt corporation bent on espionage or technology pilferage for military gain or competitive advantage may gamble and commit the crime. Presently, if caught, the worst case scenario appears to be: a public relations crisis; possible loss of the U.S. firm's facility security clearance; and perhaps, prosecution of principal U.S. citizen managers who may, or may not, have known about or willingly participated in the compromise. Logically speaking, it would not be the U.S. citizens perpetrating the crime, but rather, the representatives of the foreign interest who, acting on behalf of the foreign parent or its government, might employ clandestine methods to acquire the target information. If the technology were valuable enough, the consequences described above might present a covert operations risk worth taking. If initially undetected, the foreign interest could cover its tracks by selling or dissolving the company. More importantly, if detected, such a conspiracy would likely

result in prosecution of the U.S. citizen managers who signed the SF 312, not the representatives of the foreign interest who could be the real criminals. Having avoided espionage prosecution, the foreign investor could respond to negative press with innocent claims that the compromise was an unintentional security breach, or boldly retort the cold war is over and "anything goes" in today's increasingly tolerant environment of competitive business intelligence.

As FOCI situations become more prevalent, it will become obvious that the long arm of U.S. law must extend, if possible, to the foreign nationals or firms who stand to benefit financially, or otherwise, from their investment in U.S. high technology. Presently, a legal review is required to determine the feasibility of (a) requiring the foreign investor(s) to be cleared or clearable in their own country pursuant to bilateral security agreements; (b) to have the representatives of the foreign interest execute a SF 312 or like document as a part of their security arrangements with the U.S. government; and, (c) to structure a legal framework such that the foreign investor(s) or their representatives can be prosecuted under existing or improved U.S. espionage statutes for violation of those arrangements. If legally practical, such proactive enhancements would improve, through deterrence, the enforcement of FOCI security policy. From a reactive perspective, given a compromise, the U.S. government would be in a better position to impose its justice system on guilty foreign nationals.

11. Personnel Security

In recent years the Office of the Secretary of Defense has facilitated significant improvements in international cooperation on security matters among NATO and other allies through such mechanisms as the Multinational Industrial Security Working Group. An excellent example is the Foreign Visit System which uses technology to electronically transmit personnel security clearance data among cooperating countries on a government-to-government basis for such requirements as attendance at classified meetings and performance on Foreign Military Sales programs.

Transmission of classified visit requests which previously took 45-70 days to process are now completed in a few hours.

Use of the Foreign Visit System is not limited to international cooperative arms programs. For example, DoD security regulations (1991) provide for the granting of a Limited Access Authorization (LAA) at the CONFIDENTIAL or SECRET level to a foreign national requiring access to classified information in connection with the granting of a facility clearance to a firm in the U.S. under foreign ownership, control, or influence. In these cases the Foreign Visit System is used to obtain a security assurance from the person's country of origin to document that the individual has a clearance in that country at a similar level to the U.S. classified access requirement. Persons granted an LAA sign a SF 312, which is interesting given the espionage prosecution issue addressed above.

While the concept behind the Foreign Visit System and the security assurance process are recognized as valuable by all participating governments, unfortunately the U.S. does not use the system to its full potential for FOCI cases. DoD uses the process when issuing LAAs to foreign nationals who serve in executive positions of firms cleared under a Reciprocal facility clearance, perhaps because of the large volume of foreign disclosure decisions required by such arrangements. However, when foreign representatives hold key positions as "Inside" Directors in FOCI firms cleared under a Special Security Agreement, the DoD does not obtain a security assurance or grant a LAA. The Inside Directors may not require access to classified material, but in their position of trust and influence at a corporate board level, the security assurance and SF 312 Non-Disclosure Agreement seem like prudent measures. At least then, they would have acknowledged the espionage statutes and their responsibility to protect classified national security information.

12. Security Awareness, Training and Education

Few policymakers or government and industry security professionals understand the complexity of FOCI issues or policy. Seemingly fewer procurement officials understand the subject matter or realize cleared foreign-owned firms are chartered in the U.S. (Alderman, 1990, February 22), employ U.S. citizens, and are subject to U.S laws and regulations. Consequently, a xenophobia exists that is a product of the widespread ignorance of the intricacies of

Voting Trusts, SSAs, and NIDs, etc. This phobia can be compared to the fear impacting many adults who find themselves forced, against their will, to adjust to the computer age. The media, intent on selling news copy, does a disservice to casual observers by adding confusion with misleading, yet intriguing stories that suggest ulterior motives and industrial espionage. Clarifying facts on the policy, threat, risks, and countermeasures are lost amongst the insinuations of evil intentions by foreign investors. Therefore, as with the computer literacy problem, the natural reaction to a FOCI problem, in or out of government, is to avoid the issue. Responses in government range from protectionist policies in the Legislative and Executive Branches, to unfortunate procurement decisions eliminating viable foreign-owned U.S. firms from supplier lists resulting in stifled competition and the loss of American jobs, to ineffectual oversight by industrial security personnel who avoid the subject during audits.

Inside the foreign-owned firms, Trustees, Proxies, and Outside Directors, often with little or no training and even less understanding of what is expected of them, are thrust into an important role that has security and fiduciary responsibility. Company employees feel frustration and doubt about the firms future when established customer relationships become strained because they are suddenly treated as foreigners, even though they have not changed citizenship. Representatives of the foreign parent may

experience the greatest shock as they adapt to being viewed as second class vendors in an increasingly competitive "buy American" defense business culture. Having often invested millions of dollars for a foothold in the enormous U.S. military market, this makes for a difficult adjustment.

Education and training needs for FOCI stem directly from the same cultural transition occurring in non-defense sectors brought on by globalization and the swift expansion of international markets. It may be more difficult for Americans to adjust to international markets and competition than executives from other nations because, comparatively, the domestic market has been so bountiful for so long. Now, in a post cold-war world the defense industry is not quite as lucrative. Competition for fewer defense dollars is heating up, major players are merging or folding, and the technological prominence enjoyed by U.S. industry is fading as capable foreign sources emerge. Protectionist survival tactics seem to be the first reaction in government and industry. Eventually, however, U.S. manufacturers find themselves rising to the challenge of global economic war and, as demonstrated by the auto industry, producing better widgets for sale in overseas markets. As this globalization metamorphosis happens, understanding of FOCI issues will increase. To help the process along so that government and industry are equipped to handle the inevitable increase in FOCI issues, specific education and training gaps must be filled.

A basic understanding of national foreign investment policy is the first education and training requirement. Building on a solid foundation of why the U.S. chooses to encourage foreign investment as part of its national economic strategy, it would be beneficial to eliminate the mystery surrounding FOCI policy. This could be done by presenting FOCI adjudication as a process which has been reduced to understandable concepts like threat, risk, and security options. Rather than attempt to teach a skeptical audience the finer points of Voting Trust/Proxies, SSAs, and NIDs, etc., which are often perceived to be as complicated as the inner workings of a computer, it would be more effective to take a simplistic approach.

Specific FOCI training and education requirements include a course for Trustees, Proxies, and Outside and Officer Directors on their fiduciary responsibilities and government security watchdog role. This training should be a prerequisite to assuming such a position and should, at minimum, include a review of the role of the Defense Security Committee, the Facility Security Officer, the Export Control Officer, as well as security procedures like the foreign parent Visitation Agreement. The government's expectations regarding oversight of the U.S. operations and the requirements of an annual compliance report should also be explained.

In a fashion similar to the training DoD makes available to security professionals on handling classified

material, a course is needed for the Facility Security Officer of a firm that has come under FOCI to clarify policy and detail acceptable standard security practices. Such a course should include operational implementation of a FOCI visitation agreement, and the control of other forms of voice and data communication. The course should provide examples of employee security awareness programs directed at FOCI situations and an effective working relationship between the Security and Technology Control Officers. A variation of the course should be made available to Facility Security Officers of U.S.-owned firms who find themselves involved with FOCI firms in classified contract matters.

In the government, policy and procurement officials require a different type of training. They do not necessarily need to know the mechanics of administering a FOCI agreement, however, they should understand the insulation or isolation provided by the various instruments. Assuring effective FOCI agreement administration should be left to the government's industrial security inspection cadre who need still another type of training. They should know something about corporate organizational structures in order to monitor the variety of communications occurring between a parent and its subsidiary. Certainly all companies are not the same, however, some types of communication exchanges are consistent like: strategic marketing plans; profit and loss reports; capital and expense budgets; sales volume and backlog; bid and proposal activity; and proposed

alliances, joint ventures, acquisitions. Much of this information is only sensitive to the company and does not threaten classified or export-controlled technology. In addressing the technical matters, inspectors should understand how to probe at interactions occurring through avenues like technical libraries, program reviews, or joint ventures that require Department of State or Commerce approved technical assistance or manufacturing license agreements. To properly safeguard sensitive technology, the government security representative must understand how such arrangements are organized.

Education and training requirements specified above are not unique to the handful of foreign acquisitions. As indicated, globalization of the defense market through international teaming, consortiums, joint ventures, etc., provide ample justification for creating education courses geared to the needs of each group. If everyone understands the issues, the problems should soon dissipate.

**C. "Plan" Step Three: Envisioning an Improved NISP
FOCI Security Countermeasures Process**

Pausing to revisit the Deming PDSA theoretical model, we recall that Scherkenbach (1991) points out that Step Three is where an operational definition of the opportunity for process improvement identified in Step One is defined by creating a vision of the improved process. It is similar to Step Two in that a flow diagram is developed, but this time the process improvements are incorporated. In accomplishing this task it is important to acknowledge that in the complicated process of FOCI adjudication, there are numerous, often competing voices exerting pressure in order to influence the outcome. To achieve consensus that the new process is an improvement over the old, the new process vision must incorporate the policy objectives of most, if not all, the voices. The following is an attempt to merge those voices.

Starting with the goals and objectives of the NISP, and recognizing the complexities of the FOCI threat environment, the NISP FOCI security countermeasures process must be threat driven, cost effective, and flexible. Building on the positive and negative aspects of the current policy discussed in the preceding analysis, obviously it must safeguard classified and export-controlled national security information assets possessed by FOCI firms. To be fair from an international relations perspective, it must be consistent with National Disclosure Policy (NDP) and General

Security of Information Agreements (GSOIA) with foreign nations. To be economically attractive, it must be consistent with national foreign investment policy goals while protective of the U.S. employment base. From the perspective of the military, it must satisfy defense procurement needs for leading-edge technology and availability in time of war, yet facilitate R&D burden-sharing among international allies. Simultaneously, it must be tolerant of the competitive position of industry and eliminate impractical facility clearance limitations that stifle competition. It must be cognizant of the realities of multinational corporations which acquire businesses around the world to establish an international market presence. Finally, it must be adaptable to a dynamic FOCI scene in a rapidly changing global economy. A graphical representation of a process that attempts to incorporate all these requirements is shown in Figure 3.3.

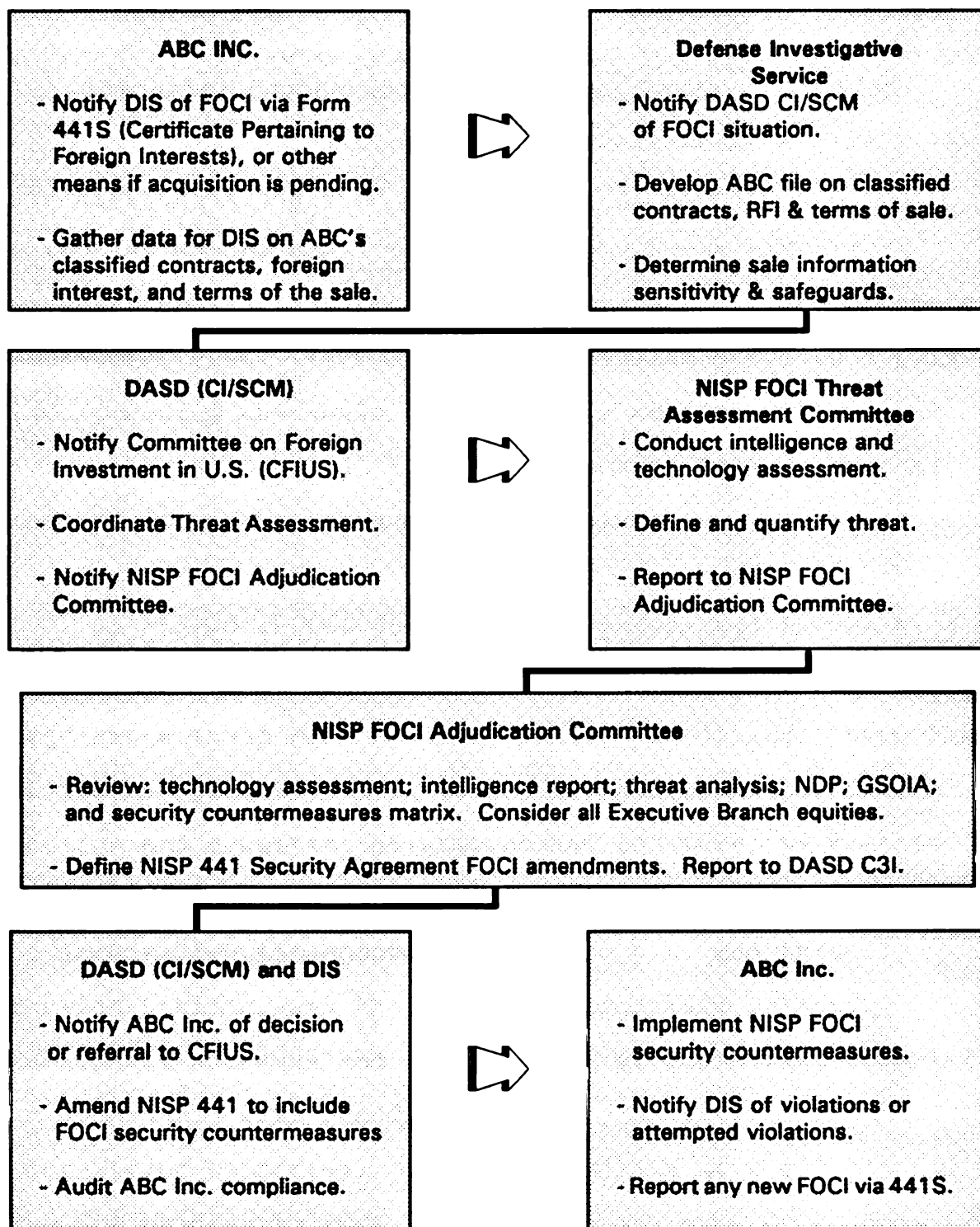


Figure 3.3

NISP FOCI Adjudication Process Model

D. "Plan" Step Four: Scoping the NISP FOCI
Security Countermeasures Process Improvement Plan

In implementing Step Four of Scherkenbach's (1991) description of the PDSA methodology, it appears the most effective way to scope recommendations for a NISP FOCI Security Countermeasures Process Improvement is to create a Management Plan. Part One of this section provides a plan incorporating the logic behind policy recommendations. Part Two provides an actual NISP FOCI Security Policy proposal incorporating the enhancement objectives.

1. Management Plan

As stated in the discussion of proscribed information (Section B-8), successful transition to a new process requires a sound FOCI security policy foundation. Step One of the Management Plan is to get all concerned parties, foreign and domestic, government and industry, to realize that the foundation is already in place. General Security of Information Agreements between the U.S. and friendly foreign nations, and the National Disclosure Policy facilitate exchange and safeguarding of classified material in accordance with standards mutually acceptable to the cooperating countries. The applicability of the GSOIA and the NDP process to FOCI adjudication and countermeasures planning must be promulgated domestically by U.S. security policy revision and established internationally through a forum like the Multinational Industrial Security Working Group. These mechanisms must be recognized as the basis of

an equitable policy on the release of classified material, including "proscribed" information, to foreign owned, controlled, or influenced U.S. companies in the NISP. For example, if the NDP and GSOIA between the U.S. and the United Kingdom or Canada allow release of proscribed COMSEC or Restricted Data to those governments, but such is not the case with Japan or France, that would be the basis for adjudication decisions regarding cleared U.S. firms with FOCI stemming from those countries. As the NDP and GSOIA are altered to compensate for changes in the international political climate; facility clearances, access requirements, threat, risk, and compensating security countermeasures could be reviewed in the affected firms.

Step Two of the Plan, perhaps the most important step, involves revamping the FOCI National Interest Determination process. Pursuant to the NISP Threat Working Group goal of creating a Catalogue of Threat Assessments (Section B-6a); the legislation of the 1993 Congressional Defense Authorization Conference (1992); and, organized by the White House endorsed DoD/CIA Joint Security Commission on future security, intelligence, and counterintelligence requirements (White House, 1993, May 26 and NSI Advisory, 1993, July); an interagency FOCI Threat Assessment Committee (FOCI/TAC) should be established to conduct effective National Interest Determinations of defense-critical technologies. In accordance with the directions of Congress, the capabilities of such entities as the Defense Intelligence Agency, the

Army Foreign Technology Science Center, Naval Maritime Center, and the Air Force Foreign Aerospace Science and Technology Center should be employed in this process. As stated in the examination of FOCI intelligence, threat assessment and risk analysis (see pages 77-78), the traditional "exclusive" versus "non-exclusive" boundaries of responsibility should be altered to allow for a more integrated and comprehensive foreign and domestic intelligence product. To be effective, the NID must not be an affirmation of procurement needs, but rather, include:

- an intelligence and technology assessment;
- a risk analysis and quantification of threat; and,
- a definition of appropriate security countermeasures.

Certain tools, such as the DIA initiated NISP FOCI database, and an unambiguous Executive Branch NISP 441S "Certificate Pertaining to Foreign Interests" standard are necessary. Taking advantage of modern technology, the usefulness of the database could be enhanced by creating it as a secure distributive processing network that uses "Contractor and Government Entity" code numbers as user identification, thus allowing timely 441S data entry and update by industry. Encryption, password protection, and appropriate software security controls would be mandatory to satisfy industry database accuracy and integrity concerns. Access must be strictly controlled in the NISP organization structure and intelligence circles because it might contain company private or sensitive securities-related information.

Step Three of the Plan is to create an interagency NISP FOCI Adjudication Committee (FOCI/AC) in one of three ways. One is to expand the charter of the National Disclosure Policy Committee (see page 88) to include FOCI adjudication. Another, would be to create a FOCI Adjudication Subcommittee of the National Disclosure Policy Committee that is linked to the NISP oversight structure when it is formalized. A third option would be to reorganize and enhance the CFIUS investigative body with leadership from, and more direct links to, the intelligence and security communities. Even if it is managed elsewhere, the FOCI/AC would still provide input to the CFIUS in extreme threat cases. Regardless of how it was constituted, the purpose of the FOCI/AC would be to evaluate the technology and threat assessments, intelligence reports, and risk analysis provided by the FOCI Threat Assessment Committee to determine appropriate security solutions for defined levels of threat in keeping with the NDP and GSOIA. The FOCI/AC must be interagency to ensure the facility clearance is acceptable to all departments and agencies who use the products or services of the contractor in the NISP. For instance, the CIA or some other agency might request certain unique requirements due to classified or covert relations with the supplier. Alternatively, that agency might abstain from deliberations if it does not contract with the firm. In any case, FOCI/AC deliberations should be patterned after the CIA model with intelligence, legal, acquisition, and security input into decisions.

Step Four is to make sure the FOCI/AC has available, not only the products of the FOCI TAC, but the current NDP, the GSOIA with foreign nations, the latest Delegation Disclosure Letters, and some guidelines such as those detailed in Figures 3.4 and 3.5 below. The guidelines, developed by government and industry security professionals, and updated in the NISP security regulations when technology or methodology advancements dictate, would provide a menu of options for negation or mitigation of risk associated with particular levels of foreign involvement.



Figure 3.4

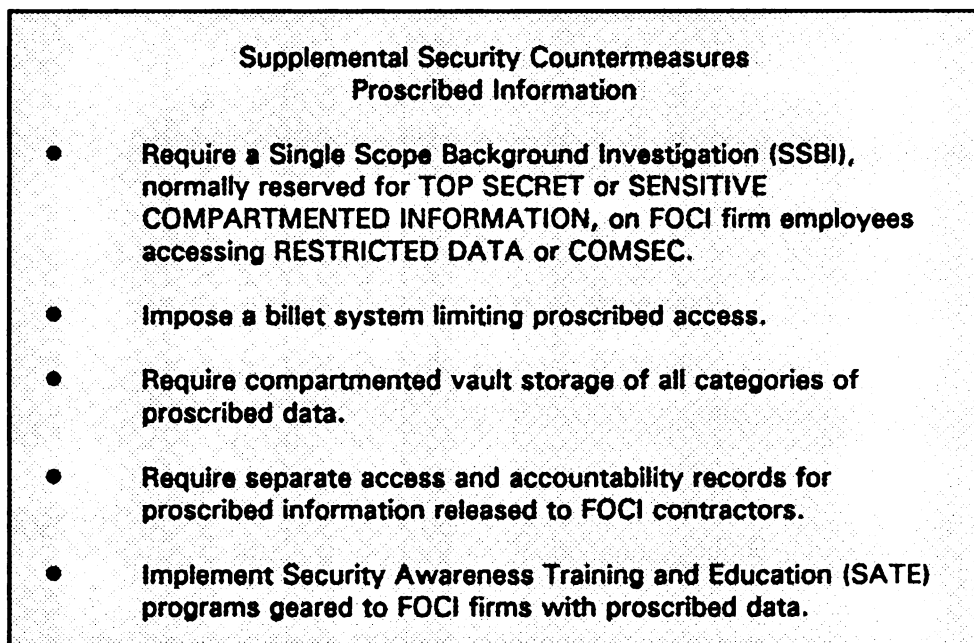


Figure 3.5

FOCI Adjudication Guidelines, Part 2

Given the appropriate tools for adjudication, it may be possible over time, for the NISP FOCI/AC to develop a Threat Assessment Matrix such as that depicted in Figure 3.6. As the adjudication process is refined, beneficial cost to both the government and industry could be quantified. Additionally, it may be possible to expedite adjudication as security countermeasures for similar threat scenarios prove their effectiveness in the oversight and compliance portion of the NISP. Time and money for adjudication and security countermeasures planning could be saved by government and industry. Foreign investors would also have an upfront, clear understanding of what would be expected of them should they acquire a firm, rather than wondering what deals can be struck during the FOCI agreement negotiation process.

THREAT	SECURITY COUNTERMEASURE	GOVERNMENT COST	INDUSTRY COST
"OWNERSHIP" FOCI from a National Security Threat List (NSTL) country.	Block sale via Exon- Florio and CFIUS.	Threat Assessment, adjudication, & CFIUS.	Not Applicable if sale is blocked.
Majority friendly foreign government equity.	Block sale via Exon- Florio and CFIUS.	Threat Assessment, adjudication, & CFIUS.	Not Applicable if sale is blocked.
Minority friendly foreign government equity.	Block sale via Exon- Florio and CFIUS.	Threat Assessment, adjudication, & CFIUS.	Not Applicable if sale is blocked.
Majority friendly foreign corporate investment(s) in equity up to, and including 100% stock ownership.	Block sale if high threat. If not: modify 441 like a Proxy, or allow minority RFI on Board; create DSC; Visitation SPP; NDP/GSOIA dictate proscribed data release.	Threat Assessment, adjudication, & counter- measure planning costs.	Proxy/Outside Director salary, DSC travel, Visitation SPP admin and other physical or procedural security costs for "Proscribed" supplemental controls.
Multiple friendly foreign investors control a majority of the equity.	Same as above.	Same as above.	Same as above.
Portfolio investment (friendly) of less than 10% of stocks/bonds.	Create DSC & enhance Proscribed data security as required.	Countermeasure planning costs only.	Possible DSC costs and Proscribed data supple- mental control costs.

Figure 3.6 (Part 1)

Conceptual example of a FOCI Threat Assessment Matrix

THREAT	SECURITY COUNTERMEASURE	GOVERNMENT COST	INDUSTRY COST
<p>"CONTROL"</p> <p>Foreign national representation on the corporation's Board of Directors.</p>	<p>Security Assurance on foreign national, SF 312</p> <p>"Non-disclosure Agreement" and a Limited Access Authorization with "proscribed" access per NDP/GSOIA.</p>	<p>Minimal cost of security assurance or further background investigative work as required.</p>	<p>Not Applicable.</p>
<p>Indebtedness to a foreign-controlled lending institution.</p>	<p>Alternative finance plan as required.</p>	<p>Research of existing data on foreign control of lending institution.</p>	<p>Alternative finance plan costs if required.</p>
<p>"INFLUENCE"</p> <p>Large foreign customer base or supplier dependence for Militarily Critical Technology.</p>	<p>Investigate criticality of supplier and identify alternate sources for small parts if possible.</p> <p>Create DSC & customer visit control SPP.</p>	<p>Threat Assessment as required.</p>	<p>Possible DSC costs for travel & administration, plus source evaluation and selection costs if domestic sources are deemed prudent.</p>
<p>Alliances, joint ventures, license agreements, etc.</p>	<p>Create DSC, & enhance emphasize export control compliance.</p>	<p>Threat Assessment as required.</p>	<p>Possible DSC costs & SATE costs for better export control.</p>

Figure 3.6 (Part 2)

Conceptual example of a FOCI Threat Assessment Matrix

Step Five of the Management Plan incorporates another innovative approach to FOCI risk management. The terms Reciprocal Facility Clearance, Voting Trust Agreement, Proxy Agreement, and Special Security Agreement would be eliminated. As indicated, they have taken on a life of their own, partly based on fact, mostly on myth. Instead of the options listed, the process would revert to the original DD 441 concept, however, it would be called a NISP Form 441 "Security Agreement." Specific security countermeasures designed to mitigate the effects of FOCI that were prescribed by the FOCI Adjudication Committee after its consultation with the FOCI Threat Assessment Committee would become the terms and conditions of amendments to the NISP 441 Security Agreement. NISP 441 FOCI amendments might be substantially similar to those in the agreements mentioned. For instance, some cases might require transfer of the voting rights for stock to government approved Proxies. Virtually all majority ownership cases would require such countermeasures as controls on foreign parent visitation, and the creation of a Defense Security Committee, or Executive Security Committee in the NISP. In essence, the most efficient and effective ingredients of current agreements, along with additional proscribed information security enhancements would be factored in as amendments to the standard NISP Form 441 as dictated by a National Interest Determination (NID) risk analysis consistent with the NDP and the GSOIA. The main difference is outside

observers would only be informed that the firm has a valid facility clearance with access limitations pursuant to the NDP. Program specific NIDs for proposal requests would not be required, saving countless manhours in government and industry, and permitting maximum competition consistent with federal procurement regulations.

Step Six of the Management Plan would be to conduct a legislative review to investigate the practicality of prosecuting the representatives of the foreign parent for willful violation of the NISP 441 under existing or improved espionage laws. Additionally, such a review should determine if a Standard Form 312 Non-Disclosure Agreement can be applied to a representative of the foreign interest. If so, as appropriate, the U.S. government should request a security assurance from the foreign nation where the FOCI stems, and process "Inside" Directors for a Limited Access Authorization (LAA) as Owners, Officers, Directors, and Executive Personnel of the FOCI firm, both as a deterrent and as an espionage prosecution tool.

The FOCI security policy which follows in Part Two of this section embraces the improvement goals of this Management Plan and the NISP by providing an Executive Branch standard that reduces government and industry security costs while improving protection of classified information in FOCI firms, thus resulting in a more efficient and effective national security posture.

2. NISP FOCI Security Policy Proposal

SECTION 1. Facility Security Clearance (FCL) Processing

1.0 General

1.1 Processing the FCL

1.2 Personnel Clearances Required in a FCL

1.3 Personnel Clearances Concurrent with a FCL

1.4 Exclusion Procedures

1.5 Issuance of the FCL

1.6 Interim FCLs

1.7 Parent-Subsidiary FCLs

1.8 Multiple Facility Organization (MFO) Clearances

1.9 Consultants

1.10 Verification of Clearance and Safeguarding Capability

1.11 Termination of the FCL

SECTION 2. Foreign Ownership, Control, or Influence (FOCI)

2.0 General

2.1 Policy

2.2 Notification

2.3 Threat Assessment

2.4 National Interest Determination

2.5 Methods to Negate or Reduce FOCI Risk

2.6 Board of Directors

2.7 Executive Security Committee

2.8 Technology Control Plan

2.9 Visitation by Foreign Interests

2.10 Annual Certification and Review

2.11 Compliance

SECTION 1. FACILITY SECURITY CLEARANCE (FCL) PROCESSING

1.0. General.

This section establishes standards for the granting and continuation of a contractor facility security clearance (FCL). A FCL is an administrative determination that a contractor is eligible, from a security viewpoint, for access to classified information. Contractors may not apply for their own FCL, nor request that their clearance be raised to a higher level. Only a government agency or a currently cleared contractor may request that an uncleared contractor be granted a FCL, or that an existing facility clearance be upgraded. Firms must meet the following eligibility requirements for a FCL:

- a. The contractor must need access to the classified information in connection with a legitimate U.S. government requirement.
- b. The contractor must be organized and existing under the laws of any of the fifty United States, Puerto Rico, or a U.S. possession or trust territory. Approval from the Deputy Director (Industrial Security), Headquarters, Defense Investigative Service is required before a FCL is processed on behalf of any government agency participating in the NISP.
- c. The contractor must have a reputation for integrity and lawful conduct in business dealings, and its key managers must not be barred from working on U.S. government contracts.

- d. The contractor must not be under foreign ownership, control, or influence (FOCI) to such a degree that a FCL would be inconsistent with national interests.

1.1. Processing the FCL.

The Cognizant Security Office (CSO) for the area in which the facility is located will advise and assist the contractor during the FCL process. At a minimum, the firm must:

- a. Execute a "NISP Security Agreement" (NISP Form 441), or "Appendage to the NISP Security Agreement" (441-1).
- b. Submit a "Certificate Pertaining to Foreign Interests" (NISP Form 441S promptly when under initial consideration for a facility security clearance; and:
 - (1) when there are significant changes to the form;
 - (2) when requested to do so by the CSO;
 - (3) annually in conjunction with scheduled facility security inspections.

Commercial, financial, and company "confidential" information provided to the government is presumptively proprietary and shall be protected from unauthorized disclosure and handled on a strict need-to-know basis.

- c. Process key management employees for a personnel clearance in connection with the issuance of the FCL.
- d. Appoint a U.S. citizen as the Facility Security Officer who shall supervise implementation of the requirements of the NISP applicable to the firm's operations.

1.2. Personnel Clearances (PCL) Required in a FCL.

Certain individuals who control the management of the

facility through stock ownership, proxy voting rights, majority ownership of securities, or by some other method that affects the appointment and tenure of officers, directors, or principal management personnel, must be processed for a PCL in connection with the FCL. Normally this involves the owners, officers, directors, partners, regents, trustees, or executive personnel.

a. Corporations, Associations, and Nonprofit

Organizations. The chairman of the board, all principal officers, the management official in charge at the facility, and the FSO shall always be cleared at the level of the FCL.

- (1) Other officers, not requiring access to classified information or occupying positions which enable them to adversely affect policies or practices in the performance of classified contracts, do not require a PCL, provided the organization complies with the exclusion procedures in paragraph 1.4.
- (2) Other officers who require access to classified information, but at a lower level than the facility clearance, may be cleared at that level, provided they do not occupy positions which enable them to adversely affect policies or practices in the performance of the higher level classified contracts, and the organization complies with paragraph 1.4.
- (3) Directors who require access to classified

information must be cleared. However, those who do not, and who do not occupy positions which enable them to adversely affect policies or practices in the performance of classified contracts, do not require a PCL. A director who also serves as a principal officer shall be cleared. If the organization conducts meetings with a pro tem chairperson or by a rotating chair, all board members who are eligible for or who could sit as chair shall be cleared. For all uncleared directors, the organization shall comply with paragraph 1.4. If the board delegates its responsibilities to a legally constituted executive committee, its members shall be cleared, or excluded per paragraph 1.4.

- b. Sole Proprietorships. The owner, all officers, if applicable, the management official in charge, and the FSO shall always be cleared at the level of the FCL.
- c. Partnerships. All general partners, the management official in charge, and the FSO shall always be cleared at the level of the FCL, or excluded as follows:
 - (1) Partners not requiring access to classified information or occupying positions which enable them to adversely affect policies or practices in the performance of classified contracts do not require a PCL provided the general partners comply with paragraph 1.4.

(2) Partners requiring access to classified information at a lower level than the facility clearance shall be cleared at that level, provided they do not occupy positions enabling them to adversely affect policies or practices in the performance of higher level classified contracts, and the general partners comply with paragraph 1.4.

(2) If the partnership delegates certain of its duties and responsibilities to a legally constituted executive committee, all committee members shall be cleared in connection with the FCL. Other non-executive committee member general partners may be excluded provided the committee has full executive authority to exercise management control and supervision for the partnership, and with respect to these other partners, the organization complies with paragraph 1.4.

d. Colleges and Universities. The chief executive officer, executive personnel, the management official in charge, and the FSO shall always be cleared in connection with the FCL.

(1) Those other officers or officials who are specifically designated by the board of regents, board of trustees, board of directors, or similar executive body, in accordance with the institution's requirements, as having the authority and responsibility to negotiate,

execute, and administer classified contracts, shall be cleared. The institution shall furnish the CSO a copy of such designation of authority, and thereafter as changes occur. If this requirement is not met, all officers shall be processed for PCL's in connection with the FCL.

- (2) Regents, trustees, or directors, not requiring access to classified information and not occupying positions enabling them to adversely affect the policies or practices in the performance of classified contracts shall be excluded. If the college or university conducts meetings with a pro tem chair or by a rotating chair, all board members who are eligible to sit as chair shall be cleared. Uncleared regents, trustees, or directors, shall be excluded per paragraph 1.4.

1.3. Personnel Clearances Concurrent with the FCL.

Contractors may also designate employees who require access to classified information during the negotiation of a contract, bid proposal or quotation pertaining to a prime contract or a subcontract to be processed for a PCL concurrent with the FCL. These may include, for instance, negotiators, accountants, clerks, engineers, draftsmen, or production personnel. An FCL is not dependent on the PCL of such employees, and changes in such employees will not affect the status of an FCL.

1.4. Exclusion Procedures.

Those officers, directors, partners, regents, and trustees who, pursuant to paragraph 1.3, can be excluded altogether from the requirement for a PCL, or who can be cleared at a level below the FCL may be excluded by formal action of the board of directors or similar executive body affirming the following as appropriate: Such officers, directors, partners, regents or trustees (designated by name) shall not require, shall not have, and can be denied access to all classified information (or specific higher-level(s) of classified information) disclosed to the organization. They do not occupy positions enabling them to adversely affect policies or practices in the performance of classified contracts. This action shall be made a matter of record in the minutes of the board of directors, partnership, board of regents or trustees, or similar executive body. A dated copy of the minutes, identifying the contractor's name and address shall be furnished to the CSO.

1.5. Issuance of the Facility Clearance.

Upon satisfactory completion of the above actions, the firm will be notified by a "Letter of Notification of Facility Security Clearance" (NISP FL 381-R) of the level of FCL.

- a. A FCL is valid for access to classified information only at the same, or lower, classification level as the FCL, i.e., a contractor with a FCL at the SECRET level would be eligible for access to SECRET and CONFIDENTIAL information, but not to TOP SECRET information.

- b. The fact that a contractor has qualified for, or has been granted, a FCL shall not be used for advertising or promotional purposes. However, in the recruitment of an employee for a specific position which will require a personnel clearance pursuant to U.S. Government requirements, a contractor may include the following statement in its employment advertisements: "Applicants selected will be subject to security investigation and must meet eligibility requirements for access to classified information."
- c. In addition to a FCL, before contractors are eligible for custody (possession) of classified material, they must have storage capability approved by the CSO.

1.6. Interim FCLs.

The CSO may grant an interim FCL pending completion of the full investigative requirements. Interim TOP SECRET FCL's are valid for access to TOP SECRET information, and interim SECRET FCL's are valid for access to SECRET information. Interim FCLs are not valid for COMSEC, Restricted Data, NATO, Sensitive Compartmented Information, or Special Access Program information.

1.7. Parent-Subsidiary Facility Clearances.

When a parent-subsidiary relationship exists between two companies, they are separate legal entities and will be processed individually for a FCL. Generally, the parent must have a FCL at the same, or higher level, as the subsidiary. The CSO shall determine whether the parent is

to be cleared or excluded from access to classified information based on the level of involvement in tasks or services essential to contract performance. If a parent and any of its cleared subsidiaries are collocated (occupying the same or adjacent office space), a written agreement to utilize common security services may be executed by the two firms, subject to CSO approval.

1.8. Multiple Facility Organization (MFO) Clearances.

When a company is composed of multiple facilities existing as a single legal entity, the home office facility (HOF) must have a clearance at the same, or higher, level as any other facility in the MFO. The "Security Agreement" (NISP Form 441) shall be executed by the HOF and an Appendage (NISP Form 441-1) shall be executed for other cleared locations. A copy of the Form 441 and each 441-1 shall be furnished to all facilities in the MFO and to each CSO concerned. The HOF is responsible for ensuring compliance with the terms of the Security Agreement and this manual for all classified contracts in the MFO, at cleared and uncleared facilities where cleared personnel are located.

- a. A single SPP may be issued within the MFO and amended as necessary for each cleared location's operations.
- b. If approved by the CSO, the HOF may establish one or more principal management facilities (PMF) for defined geographical or functional areas. The PMF shall hold the PCL Letters of Consent and be responsible for PCL administration for employees located in that area.

- c. The HOF or PMF shall provide reports to its CSO of all uncleared locations where cleared employees work.
- d. When cleared employees are located at uncleared locations, the HOF shall designate a cleared management official who shall:
 - (1) conduct recurring briefings for all cleared employees and provide written confirmation of the briefings to the HOF.
 - (2) implement the reporting requirements of the NISP for all cleared employees and furnish reports to the HOF or PMF for further submittal as required.
- e. If there is no cleared management official available at the uncleared location, the FSO of the HOF or a PMF may conduct the recurring briefings and retain a record of the briefing until after the next CSO inspection.
- f. All classified visit requests for cleared employees at uncleared locations shall be sent by the HOF or PMF.

1.9. Consultants.

A consultant is a person or a firm engaged to provide professional or technical advice to a contractor who requires access to classified information in the performance of those services. Consultants are not eligible for access to classified information outside the U.S. and its trust territories and possessions unless on official travel status of not more than 90 consecutive days in any 12-month period. Unless advised by the DIS, self-employed consultants do not require an FCL regardless of the business structure.

Consultants are categorized as follows:

- a. **Type A Consultant.** The consultant will not possess classified material except at the hiring contractor's cleared facility, at a government installation, or while on authorized visits. The consultant and the hiring contractor shall jointly execute a consultant certificate which sets forth their respective security responsibilities. The consultant must have a PCL, but a FCL is not required. Each contractor shall be the user of the services offered by the Type A Consultant it sponsors for a PCL. A Type A consultant is considered an employee of the hiring firm and a NISP Form 254 Security Classification Specification is not required.
- b. **Type B Consultant.** The consultant will be required to possess classified material at his or her place of business and will have full responsibility for security of the classified material. The consultant must have a FCL for the location where classified material is possessed and consulting services are performed. A Type B consultant is a subcontractor to the hiring contractor and a NISP Form 254 is required.
- c. **Type C Consultant.** A cleared contractor's employee who is engaged by a government agency for consulting services and will be required to possess classified information at the contractor's facility. The contractor and the employee shall execute a letter agreement which sets forth their respective security

responsibilities. The FCL and safeguarding capability of the employer is valid for a Type C consultant and a separate FCL is not required. A Type C consultant is a prime contractor and a NISP Form 254 will be issued by the government agency.

1.10. Verification of FCL and Safeguarding Capability.

Contracting activities may request verification of a contractor's FCL and safeguarding capability from:

Defense Industrial Security Clearance Office (DISCO)
Central Verifications Activity
P.O. Box 2499
Columbus, OH 43216-5006
Telephone: (614) 238-2133

Requests involving transfer of material requiring more than two cubic feet of storage, commercial carriers, freight forwarders, or certification of the FCL and safeguarding ability to the Defense Technical Information Center, shall be forwarded to the contractor's CSO. Verifications may be requested from the Central Verification Activity or the CSO by telephone or letter. Oral confirmation normally will be provided immediately, followed by written confirmation that is valid for one calendar year from the date of issuance unless superseded in writing by the DIS.

1.11. Termination of the Facility Clearance.

- a. A FCL remains in effect until terminated by either party. Upon termination, the contractor shall return all classified material to the government or destroy it

if instructed by the CSO. The original "Letter of Notification of Facility Security Clearance" (NISP FL 381-R) shall be returned to the CSO. Classified material records, reproduction logs, visitor records, and destruction certificates shall be retained for the prescribed period, and are subject to CSO review.

- b. The DISCO Forms 560, "Letter of Consent," shall be retained for 2 years from the date of termination of the PCL, or returned to DISCO upon request. Reproduction in any manner of the DIS FL 381-R or a Form 560 shall not be made except for the necessary records of the contractor, or upon request of the government.

SECTION 2. FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE

2.0. General.

This section establishes the process for examination, adjudication, and security countermeasures development when a contractor being considered for an initial or continued FCL has a significant level of foreign ownership, control, or influence (FOCI). A firm is considered to be under FOCI when a reasonable basis exists to conclude that the nature and extent of foreign involvement is such that dominance over the management or operations of the company may result in a compromise of classified or export-controlled information, or adversely impact classified contract performance.

2.1. Policy.

- a. Foundation. National foreign investment policy, National Disclosure Policy (NDP-1), and the General

Security of Information Agreements (GSOIA) between the U.S. and friendly foreign nations provide a policy foundation for FOCI adjudication. Foreign investment in the defense industrial base is neither encouraged or discouraged, and security countermeasures to safeguard classified and export-controlled information are tailored to the threat in each case. The NDP and GSOIA facilitate exchange and safeguarding of classified information with foreign governments and firms in accordance with mutually acceptable standards.

- b. Foreign Investment Regulations. Legislation and other regulatory systems designed to prevent or control undesirable foreign investment exist elsewhere in: Section Seven of the Clayton Act, Sections One and Two of the Sherman Act, Section Five of the Federal Trade Commission Act, Section 721 of the Defense Production Act of 1950, the Securities Act of 1933, the Securities and Exchange Act of 1934, the Hart-Scott-Rodino Anti-trust Improvements Act of 1976, the Federal Communications Act of 1934, the Merchant Marine Act of 1936, Section 5021 of the Omnibus Trade and Competitiveness Act of 1988, and the International Emergency Economic Powers Act.
- c. Clearance Eligibility. Foreign-owned U.S. contractors may be eligible for a FCL, provided security countermeasures can be implemented that effectively negate or reduce elements of foreign involvement to an acceptable

level. If such measures are not possible, the contractor shall be ineligible for access to classified information, and a FCL shall not be granted, or it shall be revoked, as applicable. A facility owned, controlled, or influenced by any foreign government, governmental controlled entity, or foreign national, commercial business, or investor associated with a country on the National Security Threat List, is not eligible for a FCL.

- d. Procurement Eligibility. FCLs are only granted to companies incorporated or organized under the laws of the United States. As such, even those that are owned, in whole or in part, by foreign interests are U.S. companies and therefore subject to all U.S. laws and regulations, including the Arms Export Control Act and the Export Administration Act. As a general rule, the fact that a cleared U.S. company is under FOCI should not be deemed prejudicial to the company's eligibility to compete for classified work on an equal basis with other domestic firms. Contracting activities are responsible for ensuring that cleared U.S. firms under FOCI are not precluded from bidding on classified contracts solely because of foreign involvement. A foreign-owned U.S. contractor's eligibility to pursue certain contracts and subcontracts may, however, be restricted pursuant to the provisions of this manual and the Federal Acquisition Regulation. If

restrictions are imposed on the FCL of a contractor under FOCI, they shall be documented as amendments to the NISP Form 441 Security Agreement. Government activities and prime contractors shall be advised of such restrictions in the FCL verification letter obtained from the Central Verification Activity.

2.2. Notification.

- a. Pursuant to paragraph 1.2, contractors must notify the CSO of foreign involvement by submitting a NISP Form 441S "Certificate Pertaining to Foreign Interests." The CSO shall notify the DIS, Deputy Director (Industrial Security), when information received from a contractor via the 441S or other means, indicates that discussions or negotiations with a foreign interest or its representative have resulted, or may result, in the transfer of ownership, control, or influence.
- b. Private sector investment decisions must be made without government intervention or influence until statutory or regulatory jurisdiction is established. The rendering of advisory opinions, rulings, or assistance which could influence investment decisions, such as a prospective merger, acquisition or takeover, shall not commence until a potential seller of assets or stock has been presented with a formal purchase offer by a potential foreign investor. Government staffing of a FOCI case can commence before a purchase offer is made when a voluntary notice has been accepted by the

Committee on Foreign Investment in the United States (CFIUS) pursuant to the implementing regulations of the Department of the Treasury (31 CFR Part 800).

- c. If a contractor is determined to be under FOCI by the DIS, Deputy Director (Industrial Security), the CSO shall promptly invalidate the company's FCL and the level of approved safeguarding (storage), if any, shall not be verified.
- d. When a company with an invalidated FCL has current access to classified information, DIS shall ensure that the contractor, cognizant government security and acquisition officials, and all prime contractors of record are concurrently furnished written notice of the invalidation. Such notices shall state that the award of additional classified contracts is prohibited until the FCL has been reinstated. Current access to classified information and performance on existing contracts may continue unless notified by the government to the contrary. In FOCI cases, the primary consideration is sensitive government information and the DIS shall take whatever interim action is necessary to prevent compromise of classified and export-controlled information.
- e. If the contractor does not possess classified material, and does not have a current or impending access requirement, the FCL shall be administratively terminated or initial processing discontinued, as applicable.

- f. Within 5 working days from the date of invalidation, a case file shall be referred by the CSO to the DIS, Deputy Director (Industrial Security). The file shall include an updated NISP Form 441S, all other relevant documentation, any plan proposed by the contractor to reduce FOCI security risks to an acceptable level, and the CSO's evaluation and recommendation.
- g. The DIS shall advise the contractor that failure to adopt acceptable security measures, including any interim requirements imposed pending final resolution, may result in denial or revocation of the FCL. When consensus is reached among all parties to the Form 441 Security Agreement, and after security countermeasures are implemented, the Director, DIS shall authorize execution of a FCL. If consensus is not reached, the firm shall be advised of government appeal channels.
- h. Official rulings concerning the resolution of FOCI cases, to include the terms and conditions of the NISP Form 441 Security Agreement executed among the government, the U.S. contractor, and the foreign investor(s), shall not be publicized without government legal review, or the concurrence of the U.S. contractor and the foreign investor(s).

2.3. Threat Assessment.

- a. DIS. The Deputy Director (Industrial Security), DIS shall consider the facts of the case and, as appropriate, notify the interagency NISP FOCI Threat

Assessment Committee (FOCI/TAC) coordinated by the FOCI Adjudication Committee (FOCI/AC), a subcommittee of the National Disclosure Policy Committee.

- b. Interagency Review. The FOCI/TAC shall coordinate an interagency review of contractor foreign connections to identify matters of national security significance and provide DIS intelligence and counterintelligence support as follows:**

- (1) The FOCI/TAC shall prepare a comprehensive technology, intelligence and counterintelligence assessment.**
- (2) The FOCI/TAC shall define and quantify threat and prepare a comprehensive risk assessment concerning the foreign government(s) involved, the U.S. company, and all intermediate parent companies leading back to the ultimate foreign investor.**
- (3) The FOCI/TAC shall manage an automated database where information received from cleared contractors on the Form 441S will be centrally stored. Due to the proprietary nature of the information contained in the database, strict accountability control and dissemination procedures will be maintained to prevent unauthorized release of company sensitive or investment critical data.**

- c. Criteria. All types of foreign involvement are subject to review and must be reported on the NISP Form 441S including, but not limited to:**

- (1) Foreign interest ownership or beneficial ownership of five percent or more of the firm's securities;
- (2) Ownership by any foreign interest, in whole or in part;
- (3) Management positions held by foreign interests such as directors, officers, officers or executive personnel;
- (4) Foreign interests control or influence, or are positioned to control or influence the election, appointment, or tenure of directors, officers, or executive personnel;
- (5) Contracts, agreements, understandings or arrangements with foreign interests;
- (6) Indebtedness to foreign interests;
- (7) Any income derived from National Security Threat List countries, or income in excess of ten percent of gross income from other foreign interests;
- (8) Five percent or more of any class of the entity's securities are held in "nominee shares" in "street names" or in some other method which does not disclose the beneficial owner of equitable title;
- (9) Interlocking directors with foreign interests;
- (10) Any other factor that indicates or demonstrates a capability on the part of foreign interests to control or influence the operations or management of the contractor.

2.4. National Interest Determination.

a. **Adjudication.** Interagency examination and adjudication of FOCI considered to be of national security significance that are revealed by the FOCI/TAC is accomplished by the FOCI Adjudication Committee (FOCI/AC), a Subcommittee of the National Disclosure Policy Committee. Considering the equities of all Executive Branch activities, the FOCI/AC shall:

- (1) **Render a National Interest Determination (NID)** regarding the continuation or issuance of a FCL to a U.S. firm given the level and nature of FOCI in the case. Certain U.S. companies may be of such fundamental significance to national security that the government may not permit them to be acquired by any foreign interest. Such a position may be based on a NID that the FOCI negation measures prescribed herein would provide inadequate protection. Further, the threat posed by some foreign acquisitions, mergers, or takeovers of U.S. contractors may be so great that developing additional safeguards to protect vital technology or capabilities, may be impractical even if the contractor is not critical to national security.
- (2) **Define threat driven security countermeasures** to be detailed in amendments to the firm's NISP Form 441 Security Agreement. Generally, a FCL will be granted at the SECRET level or lower. Should the

FOCI threat increase, or a procurement opportunity materialize requiring the firm to have higher-level access, the FOCI/AC may specify amendments to the NISP 441 such as those listed below.

- b. **Criteria.** Generally, foreign ownership of a U.S. contractor under consideration for a FCL becomes a concern when the amount of foreign-owned stock is at least sufficient to elect representation to the U.S. company's board of directors or foreign interests are otherwise positioned to select such representatives (equivalent equity for unincorporated business). Foreign ownership which cannot be so manifested is not, in itself, considered significant. Insignificant foreign stockholdings are, nonetheless, analyzed to determine source and significance when considered in conjunction with other aspects of FOCI in a case. Proposed merger, acquisition or takeover cases subject to Section 721 of Title VII of the Defense Production Act of 1950 (P.L. 102-99) are processed on a priority basis. The government shall promptly identify required security safeguards to the parties of such transactions to permit negotiation and disposition within prescribed statutory timeliness. The FOCI NID rendered by the FOCI/AC shall, at minimum, consider:
- (1) The FOCI/TAC technology assessment regarding the criticality of the contractor's products or services to defense industrial base preparedness,

- mobilization, planning, or research requirements;
equipment production needs of the military; and
the needs of other departments and agencies;
- (2) The nature and extent of FOCI, and the likelihood of classified or export-controlled material compromise;
 - (3) The FOCI/TAC intelligence, counterintelligence, and threat assessments prepared on the contractor and all parent companies back to the ultimate foreign investor;
 - (4) The NDP for the country(s) from which FOCI stems;
 - (5) The existence, or lack of, a GSOIA with the country(s) from which FOCI stems; the terms and conditions of such agreements; and the foreign nation(s) record of compliance with the GSOIA;
 - (6) The classification level, or lack of, a FCL held by the foreign investor(s) in the foreign nation(s) from which the FOCI stems; and if available, the foreign investor(s) compliance record with that nation's security program;
 - (7) Loans, organization charts, annual reports, articles of incorporation, corporate bylaws, partnership agreements, and reports filed with federal agencies;
 - (8) The U.S. contractor's security posture and performance record safeguarding classified information in the NISP.

- (9) The security countermeasures that must be amended to the contractor's Form 441 Security Agreement to negate or reduce the effects of FOCI to an acceptable level;
- (10) The amount of classified information possessed, or required, by the contractor above SECRET. A FCL authorizing possession of material in the following "proscribed" categories shall not be granted to a FOCI contractor unless the NDP and GSOIA with the country(s) from which FOCI stems allow such releases on a government-to-government basis and the NISP 441 has been amended per in 2.5f below:
 - (a) TOP SECRET information;
 - (b) Restricted Data;
 - (c) COMSEC information;
 - (d) Sensitive Compartmented Information
 - (e) Special Access Program information;
 - (f) Information not releasable by U.S. Government NDP to the country(s) from which FOCI stems;
 - (g) Information for which foreign dissemination has been prohibited, in whole or in part;
 - (h) Information furnished to the U.S. Government in confidence by a third party government.

2.5. Methods to Negate or Reduce FOCI Risk.

- a. General. In FOCI cases, the NISP Form 441 Security Agreement between a contractor and the government shall become a three-party contract also binding the foreign

interest(s) to safeguard classified information in accordance with this manual. Security countermeasures designed to negate or reduce FOCI risks are detailed in amendments to the Form 441.

- b. Low Threat FOCI Cases. Low threat FOCI cases include, but may not be limited to, the following situations:
- (1) Foreign-owned or controlled stock is sufficient to elect representation on the U.S. company's board of directors, but identifiable U.S. interests own or control 50% or more of the company's voting stock; a U.S. interest not under FOCI is the largest single shareholder; and the nature, class and distribution of the minority-owned shares do not, and would not if converted, permit foreign control of company management or operations.
 - (2) Portfolio investment where foreign interest(s) own voting stock (usually less than 10%), directly or indirectly, that is insufficient to elect representation to the U.S. firm's board of directors.
 - (3) Foreign national representation, without stock ownership, on the company's board of directors.
 - (4) Insignificant indebtedness to foreign-controlled lending institution(s).
 - (5) Limited influence from foreign customers or suppliers.
 - (6) Foreign influence through alliances, joint ventures, teaming arrangements, manufacturing

license and technical assistance agreements, or other global partnerships.

- c. **Low Threat FOCI Security Countermeasures.** Barring any mitigating circumstances such as technology criticality or specific threat information, the NISP Form 441 may be amended without restriction of eligibility for any classified contract. Such amendments may include:
- (1) Identification of the foreign interest(s) and the type and extent of foreign-owned shares;
 - (2) Resolution(s) by the board of directors certifying that the foreign interest shall not require, shall not have, and can be effectively denied access to classified and export-controlled information;
(The firm must document distribution of the resolutions to corporate officials.)
 - (3) Resolution(s) signed by the foreign interest waiving any right of access to classified or export-controlled information possessed by the firm;
 - (4) Annually renewed certifications by the foreign interest that acknowledge understanding and acceptance of FOCI security policies, and pledging not to interfere with the performance of classified contracts;
 - (5) Provisions to control visits by the foreign interest to facilities possessing classified or export-controlled information;
 - (6) Annually renewed certifications by the corporate

board affirming the ongoing effectiveness of the resolution(s); or

- (7) Provisions for the board of directors to adopt further resolutions or take action to assure the government that the FCL remains consistent with the national interest.

Other measures employed concurrently may include:

physical or organizational compartmentation of classified work; modification or termination of foreign interest agreements; diversification or reduction of foreign source income; assignment of security duties to company officials; elimination or resolution of problem debt; and amendments to loan, purchase, and shareholder agreements. Low threat cases are monitored to determine if high threat security solutions are warranted.

d. High Threat FOCI Cases. High threat FOCI cases

include, but may not be limited to, the following:

- (1) FOCI stems from a National Security Threat List country;
- (2) Majority friendly foreign government equity investment;
- (3) Minority friendly foreign government equity investment;
- (4) Friendly nation foreign persons or commercial interests own or control 50% or more of the stock;
- (5) Multiple foreign investors own or control a total of more than 50% of the company's voting stock.

e. **High Threat FOCI Security Countermeasures.** Barring any mitigating circumstances such as technology criticality or specific threat information, the NISP Form 441 may be amended to include one of the following:

- (1) A resolution(s) implemented through the company's bylaws transferring all voting rights, power, and authority with respect to common voting stock (except proposals that, by statute, charter or bylaws, cannot be taken without foreign shareholder approval) to cleared U.S. citizen Outside and/or Officer Director(s) approved by the DIS.
 - (a) The foreign shareholder(s) must relinquish operational control of the company.
 - (b) Such arrangements would not restrict a contractor's eligibility for access to any category of classified material.
- (2) A resolution(s) implemented through the company's bylaws allowing only minority foreign representation during a meeting or vote of the board of directors.
 - (a) The chairman and a majority of corporate board must be cleared U.S. citizens approved by the DIS.
 - (b) Such an arrangement imposes substantial industrial security and export-control protection promulgated by the corporate board through the company's security procedures.

- (c) Representatives of the foreign interest are excluded from meetings when classified or export-controlled information is discussed.
- (c) Generally, the company's FCL is limited to the SECRET level per section 2.4b(10).
- (d) Access to proscribed information is only authorized if the country from which the FOCI stems has a GSOIA with the U.S., and NDP would otherwise allow disclosure via government-to-government channels.
- (e) Additional proscribed information safeguards deemed appropriate by the DIS (detailed below) have been implemented.

NOTE: A Contractor may not disclose classified material to its parent unless authorized in connection with a Foreign Military Sales or other approved contract.

- f. Proscribed Information Safeguards. When foreign interests sit on the corporate board or visit facilities storing proscribed information, additional safeguards may be required, such as:
 - (1) U.S. citizens requiring access to any category of proscribed information will be submitted for a Single Scope Background Investigation (SSBI) normally only required for TOP SECRET access;
 - (2) A billet system to limit exposure to proscribed information;
 - (3) Security awareness, training and education on FOCI

threats to proscribed information;

- (4) Separate access and accountability records, and compartmentalized storage for proscribed material.

g. Changed conditions. Certain conditions, such as an increased intelligence threat, noncompliance with the NISP Security Agreement, or increased national security value of the material requiring protection, may justify certain adjustments to the FOCI mitigation methods.

- (1) The Form 441 terms and conditions may be strengthened or relaxed as warranted, however, changes should be consensual among the affected parties whenever possible.
- (2) The government must establish a legally sufficient and rational basis for the security enhancements.
- (3) The contractor must develop persuasive arguments in support of any petition to the DIS to eliminate or relax FOCI security requirements.
- (4) The government shall make the final determination whether such petitions should be granted.

2.6. Board of Directors

a. General. In FOCI firms, it is especially important that the Board of Directors and other senior officials underscore the importance of the security function by personal example, by setting forth the rules, by inspecting for compliance, and by disciplining those who fall short. Independence of the U.S. Board of Directors from foreign influence is sought, while

allowing some decision-making authority concerning general operation or long term organization and direction of the contractor. Insulation or isolation of the corporate board from foreign influence may be accomplished by assigning security duties to certain directors and by limiting the authority of others.

b. Outside Directors. Outside Directors in a FOCI firm provide balance between the U.S. firm and the foreign interest. To be eligible to serve as an Outside Director, an individual must:

- (1) Be a U.S. citizen eligible for a PCL, residing in the U.S., who has been approved for appointment by the DIS, in consultation with other agencies when appropriate;
- (2) Function as a government security "watchdog" and be capable of assuming full responsibility for exercising the management prerogatives assigned to ensure that the foreign interest is effectively insulated as required by the Security Agreement;
- (3) Have no prior relationship with the U.S. company, the foreign interest, or any affiliated entity except as approved by the DIS;
- (4) Not be dependent upon their income as a director;
- (5) Certify annually, understanding and acceptance of their duties and fiduciary responsibilities when voting company stock as a Director, or as a foreign interest proxy holder or trustee;

- (6) Receive within six months of appointment, FOCI training provided by the DIS, the Department of Defense Security Institute, or other government component as necessary.
- c. Inside Director. Under certain circumstances, the foreign interest may be authorized minority representation on the Board of Directors except at meetings when classified or export-controlled information is discussed. To be eligible to serve as an Inside Director, an individual must:
- (1) Certify upon appointment, and annually thereafter, understanding of their responsibilities under the NISP Form 441;
 - (2) Sign a resolution waiving any right of access to classified or export-controlled information in the possession of the cleared contractor;
 - (3) Certify annually not to attempt to adversely influence the performance of classified contracts, or implementation of security procedures;
 - (4) Be eligible for a "Security Assurance" in the country from which the FOCI stems;
 - (5) Agree to report any violation of the Form 441;
 - (6) Execute a SF 312 Non-Disclosure Agreement to facilitate prosecution for willful violation of U.S. espionage laws.
- d. Officer Directors. As both members of the U.S. contractor's board of directors and officers of the

company, Officer Directors serve as a liaison between the cleared company and the board. These individuals are responsible for monitoring and overseeing the daily operations of the contractor to ensure that the safeguards in the Form 441 are implemented, maintained and supported throughout its duration. To be eligible to serve as an Officer Director, an individual must:

- (1) Be a U.S. citizen eligible for a PCL, reside in the U.S., and be approved for appointment by the DIS, in consultation with other NISP agencies;
- (2) Function as a government security "watchdog" and be capable of assuming full responsibility for exercising the management prerogatives assigned to ensure that the foreign interest is effectively insulated as required by the Security Agreement;
- (3) Certify, annually, acceptance and understanding of the specific security procedures established to implement the Form 441 in the contractor's security procedures;
- (4) Acknowledge by certification, the responsibility placed on officer directors by the government, as citizens with a PCL, to exercise their best efforts to ensure compliance with the NISP 441.
- (5) Ensure that an effective security awareness, training and education program is established to sensitize employees to the FOCI threat.

2.7. Executive Security Committee.

In high threat FOCI situations, and as required in low threat cases, the U.S. contractor may be required to establish a permanent committee of the company's Board of Directors, known as the Executive Security Committee (ESC). The ESC is responsible for implementation of all procedures, organizational matters, and other aspects of security and technology export-control management called for in the NISP Form 441 Security Agreement.

- a. The ESC shall consist of the Outside Director(s), and one or more Officer Directors who hold a PCL. The Chair of the ESC shall be an Outside Director.
- b. Discussions of classified and export-controlled technical matters by the ESC shall be held in closed sessions excluding the foreign interest.
- c. The ESC shall take all necessary steps to ensure compliance with the U.S. Arms Export Control Act for military goods, and with the Export Administration Act for commercial and dual-use goods.
- d. The Facility Security Officer (FSO) shall be an advisor to the ESC and shall report to its Chair.
- e. The ESC shall appoint an Export Control Officer (ECO) responsible for the development, approval, and implementation of a Technology Control Plan.
- f. FSO and ECO functions shall be carried out under the authority and with the support of the ESC.

2.8. Technology Control Plan.

A Technology Control Plan (TCP), shall be developed and implemented by the cleared contractor when deemed appropriate by the DIS. The TCP shall prescribe all security measures determined necessary to reasonably foreclose the possibility of inadvertent access by non-U.S. citizen employees and visitors to information for which an export license is required. Unique badges, escorts, segregated work areas, security indoctrination schemes, and other measures shall be included, as appropriate. The TCP shall provide a method to ensure information exchanges with the foreign interest are reviewed and approved in advance by the FSO and ECO as appropriate.

2.9. Visitation by Foreign Interests.

In high threat FOCI cases, or as required in low threat cases, the U.S. firm may be required to establish a security procedures to control visits by the foreign interest to sites possessing classified or export-controlled material. Such procedures shall include:

- a. Provisions for recording the date, place, and purpose of each visit along with the identification of the visitor(s), host and any classified or export-controlled information approved for discussion;
- b. Provisions for ESC, FSO, and as necessary ECO review and approval of visits by foreign representatives;
- c. Provisions for the FSO and/or ECO to brief the visit host on applicable security or export-control

regulations or license provisos; and,

- d. Provisions for ESC audit follow-up to ensure compliance with visitation procedures, security or export-control regulations, and the terms of the Security Agreement.

2.10. Annual Certification and Review.

- a. Annual Certification. The Chief Executive Officer and Executive Security Committee Chair shall jointly submit an annual report and certification of compliance with the NISP Form 441 to the DIS which includes:

- (1) A detailed description of the manner in which the company is carrying out its obligations under the NISP Form 441 Security Agreement;
- (2) A detailed description of changes to security procedures, implemented or proposed, and the reasons for those changes;
- (3) A detailed description of any acts of noncompliance, whether inadvertent or intentional, with a discussion of corrective actions designed to prevent reoccurrence;
- (4) A report of any changes, or impending changes, of senior management officials and the reasons for such changes; and,
- (5) Any other issues that could have a bearing on the effectiveness or implementation of the NISP 441.

- b. Annual Review. Representatives of the DIS shall meet at least annually with senior management of companies operating under a NISP Form 441 with significant FOCI

amendments to review the purpose and effectiveness of the Security Agreement and to ensure that there is a common understanding of its operating requirements to include at least a discussion of the following:

- (1) Whether FOCI security countermeasures, controls, practices, and procedures are working in a satisfactory manner, or if they warrant adjustment;
- (2) Compliance or acts of noncompliance with the approved security countermeasures, standard NISP rules, or applicable laws and regulations; and,
- (3) Necessary guidance or assistance regarding problems or impediments with practical application of the security countermeasures. Discussion shall include issues, current or projected, concerning the security of classified and export-controlled material, the effects of FOCI, and classified contract performance.

2-11. Compliance.

Failure on the part of the company to comply with the terms of any approved security arrangement may constitute grounds for termination of the NISP Form 441 Security Agreement, revocation of the company's facility security clearance, or any other legal sanction deemed appropriate.

E. "Do" Step Five: Survey of Security Professionals

1. Survey Objectives

Action step five, the "Do" phase of Deming's Cycle, is where the plan or theory is tested, preferably on a small scale with the customers. Recall that, in this study, the test consists of an opinion survey of industry security professionals whose opinions either affirm or dispute the idea that applying the PDSA model provided an enhanced FOCI security countermeasures process. Success, or quality improvement, is determined by the extent of agreement among respondents that the twelve ideas, factored into the draft NISP FOCI policy proposal in Section D.2., represent practical process improvements. Given that security professionals from FOCI firms deal with FOCI risk management issues more often than their non-FOCI firm colleagues, the survey was designed to target both groups to determine if their views would differ on a) the effectiveness of current FOCI instruments, and, b) the ideas for process improvement.

Efforts to identify security professionals representing FOCI firms to participate in the survey were hindered by the fact that the DoD treats its list of such contractors as proprietary. However, research of publicly available data addressing merger and acquisition activity in the defense industry over the last twenty years (i.e., Hanson, Pagliano, Wartzman, Defense Forecasts, and others cited), made it possible to piece together a list of firms likely to be working under DoD FOCI arrangements. For instance, Defense

Forecasts, Inc. reported the existence of approximately 40 SSAs in 1992 and discussed several of the more prominent FOCI cases. Fewer Voting Trusts and Proxies exist due to their more restrictive nature, which yields a total population of less than 100 (probably less than 75) of the more formal FOCI mitigation instruments. Data on Reciprocal clearances and Board Resolutions was also not available; however, because they have been a part of the DISP for a longer time, they likely number several hundred.

Telephonic contact of the security professionals from firms identified in the research discussed above resulted in a more refined list of 55 who indicated they were involved in FOCI agreement administration, and would participate in the survey. Security association membership rosters were used to contact another 59 large and small non-FOCI firm security professionals from the population of 11,817 (Suto, 1992) cleared by the DIS, resulting in a sample size of 114.

The next step was to mail individual letters of transmittal, along with a copy of the questionnaire in booklet form (with a return postage paid envelope) to each security professional. Beginning with the survey instrument introduction, its 15 questions (3 on demographics and 12 on process improvement ideas), and the responses received are presented in Section E, Part 2 below. Analysis of the results, the "Study" phase of the PDSA model, follows in Section F below.

2. Survey Instrument and Responses

A Quality Security Countermeasures Process for Foreign Ownership, Control, or Influence (FOCI) of United States Defense Firms in the National Industrial Security Program A Survey of Security Professionals

INTRODUCTION

The National Industrial Security Program (NISP) replaces a plethora of overlapping, often conflicting industrial security regulations with a single, coherent and integrated Executive Branch strategy to safeguard U.S. national security information. Total Quality Management (TQM) is the goal of this effort to develop an efficient and cost-effective security posture. Fiscal constraints necessitate replacement of "Cold War" risk avoidance methods with risk management processes.

One complex process for NISP architects is the risk of unauthorized technology transfer inherent in foreign ownership, control, or influence of U.S. defense contractors. Crafters of FOCI security policy in the NISP must be consistent with prevailing national foreign direct investment policy, yet they can ill afford to join the emotional political debate over the benefits and detriments of increased foreign investment in the U.S. defense industrial base. To accomplish their mission, they must avoid political squabbles and address FOCI as an increasingly important risk management issue so a quality security strategy is defined.

This survey supports thesis research of Daniel Muscat, a security professional and Michigan State University

graduate student, who employed W. Edwards Deming's "Plan, Do, Study Act" process improvement theoretical model to help detect flaws in current FOCI security strategy in order to define a quality countermeasures process for the NISP. It is designed to gather opinion data from security professionals in both foreign and domestic-owned defense firms on the merits of process improvement ideas which resulted from a critical analysis of current regulations. Results will be provided to the NISP Task Force for consideration. Your assistance in completing this survey is designed to contribute to NISP development.

The amount of time required to complete this survey is estimated at 20 minutes. Confidentiality of the opinions of individual participants is assured since names and corporate affiliations are not solicited. On request, and within these restrictions, the results of this study may be made available for review.

You indicate your voluntary agreement to participate in the survey by completing and returning the questionnaire. For convenience, a self addressed, postage paid, return envelope has been provided. Should you have any questions when completing the survey, contact Daniel Muscat at Box 88291, Kentwood, MI 49518 or call (616) 241-7607.

Consistent with milestones established for implementation of the NISP, your earliest response is most appreciated. Findings are scheduled to be summarized in early March 1994. Thank you for your support.

After the introductory section of the survey booklet above, the first two questions requested demographic data to facilitate analyzing responses by FOCI versus non-FOCI firm.

1. Which category best describes your employment status?

Select only one;

- ☐ Security professional for a U.S.-owned defense contractor (Go to question #3).
- ☐ Security professional for a foreign-owned, controlled, or influenced (FOCI) contractor as defined by the DoD.
- ☐ Other, (explain) _____

A total of 114 surveys were distributed and 77 were returned for a 67.5% response rate. Respondents included 49 (64%) from non-FOCI firms and 28 (36%) from firms with FOCI as defined by the DoD.

2. If you represent a FOCI firm, which type of security arrangement has been employed to facilitate the granting or continuance of a facility security clearance at your company?

- ☐ Voting Trust Agreement
- ☐ Proxy Agreement
- ☐ Reciprocal Clearance
- ☐ Board Resolution
- ☐ Special Security Agreement (SSA)

There were 28 FOCI firm respondents; 1 operating under a Voting Trust, 4 under a Proxy, 5 under a Reciprocal clearance, 3 under a Board Resolution, and 15 under an Special Security Agreement.

While not part of the Deming Cycle "Do" phase test of the process improvement ideas, survey question 3 solicited opinions on current FOCI risk mitigation instrument effectiveness. Respondents could choose from among Very Effective, Somewhat Effective, Somewhat Ineffective, Very Ineffective, and Unsure.

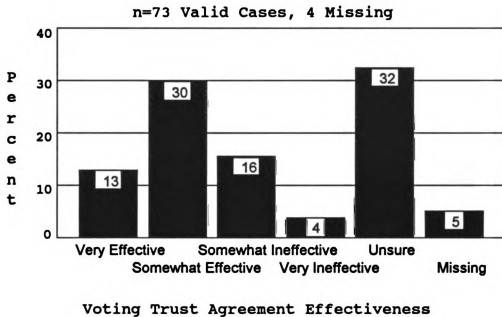
3. Scrutiny of DoD FOCI policy by Congress, the media, and others in 1992/1993 impacted efforts to objectively critique current processes while developing an efficient, cost-effective, threat-driven program for the NISP. Setting aside the opinions of others, given your professional experience, rate the overall effectiveness of the various DoD FOCI risk mitigation instruments in safeguarding national security interests, classified information, and export controlled technology from threats inherent in FOCI.

- a. Voting Trust Agreement
- b. Proxy Agreement
- c. Reciprocal Clearance
- d. Board Resolution
- e. Special Security Agreement

The results of the ratings on the effectiveness of current FOCI mitigation instruments in question 3 are detailed in Figures 3.7 - 3.11 below. To facilitate analysis of whether FOCI and non-FOCI firm respondent rating patterns differed, cross tabs were created which further break down the data into two variables, Employment and Effectiveness. Employment is defined as a FOCI or non-FOCI firm respondent. In the variable Effectiveness, the rating

categories Very Effective and Somewhat Effective were merged into one category called Effective, and the Somewhat Ineffective and Very Ineffective categories were merged into another category called Ineffective. The rating category Unsure and all Missing responses were eliminated from consideration.

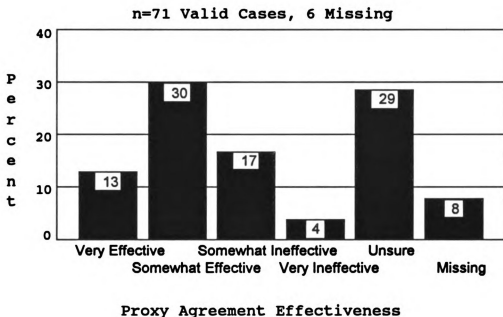
In each of the cross tabs, a Chi Square test of independence was conducted on the variables Employment and Effectiveness. A 95% confidence level with 1 degree of freedom was established as the threshold for evaluating their independence. Using these parameters, the critical value for Chi Square is $X^2(1) = 3.84$ or greater when the probability is $P = .05$ or less (95% confidence level). Consequently, if any of the Chi Square calculations resulted in $X^2(1) = 3.84$ or greater when $P = .05$ or less, it would suggest that the respondents effectiveness ratings were related to Employment.



		EFFECTIVENESS		
		Effective	Ineffective	Row Total
EMPLOYMENT	Non-FOCI Firm	20	13	33 68.8%
	FOCI Firm	13	2	15 31.3%
Column Total		33 68.8%	15 31.3%	n=48 100%
		$\chi^2(1) = 3.2$ $P = .07$		

Figure 3.7

Security Professional Ratings
Voting Trust Agreement Effectiveness

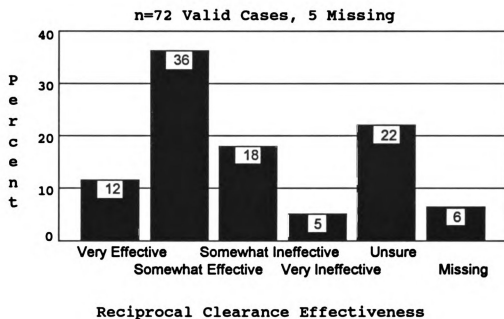


		EFFECTIVENESS		
E M P L O Y M E N T		Effective	Ineffective	Row Total
	Non-FOCI Firm	21	12	33 67.3%
	FOCI Firm	12	4	16 32.7%
	Column Total	33 67.3%	16 32.7%	n=49 100%

$\chi^2(1) = .63 \quad P = .42$

Figure 3.8

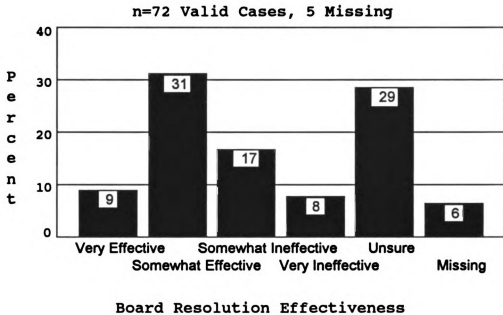
Security Professional Ratings
Proxy Agreement Effectiveness



		EFFECTIVENESS		Row Total
		Effective	Ineffective	
EMPLOYMENT	Non-FOCI Firm	23	14	37 67.3%
	FOCI Firm	14	4	18 32.7%
Column Total		37 67.3%	18 32.7%	n=55 100%
		$\chi^2(1) = 1.3$		P = .24

Figure 3.9

Security Professional Ratings
Reciprocal Clearance Effectiveness

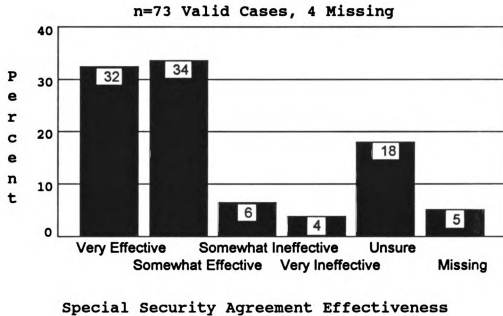


		EFFECTIVENESS		
EMPLOYEE RATING		Effective	Ineffective	Row Total
	Non-FOCI Firm	21	14	35 70.0%
	FOCI Firm	10	5	15 30.0%
Column Total		31 62.0%	19 38.0%	n=50 100%

$X^2(1) = .19 \quad P = .65$

Figure 3.10

Security Professional Ratings
Board Resolution Effectiveness



		EFFECTIVENESS		
EMPLOYMENT		Effective	Ineffective	Row Total
	Non-FOCI Firm	33	6	39 66.1%
	FOCI Firm	18	2	20 33.9%
	Column Total	51 86.4%	8 13.6%	n=59 100%
		$\chi^2(1) = .2$		P = .56

Figure 3.11

Security Professional Ratings
Special Security Agreement Effectiveness

In survey questions 4 - 15 below, the process improvement ideas which resulted from the PDSA exercise were tested. Consistent with the format above, each question is followed by a chart and crosstabs (Figures 3.12 - 3.23). For these questions, the respondents were asked to select all that apply from among Practical, Impractical, Process Improvement, No Value Added, and Unsure. The bar graph charts with each question show the percent of all responses (including Unsure) selected for each rating category.

For the cross tabs, analysis indicated a pattern where many respondents consistently chose Practical and Process Improvement, or Impractical and No Value Added. Therefore, two new variables were created, Practicality defined as Practical or Impractical, and Value defined as Process Improvement or No Value Added. To facilitate analysis of whether FOCI and non-FOCI firm respondent rating patterns differed, the variable, Employment was once again used as defined in question 3 above. Two cross tabs are presented with each question 4 - 15 to compare the variables Employment and Practicality, and Employment and Value.

In these charts and crosstabs, the number of cases varies because all respondents could check more than one response to each question, but the Chi Square rules defined on page 164 for question 3 are exactly the same. Finally, as with the crosstabs above, Unsure and Missing ratings were not considered.

PDSA TEST

Survey question 4 below, the first in the PDSA test, addressed the idea of using National Disclosure Policy and the General Security of Information Agreements as the foundation for FOCI policy.

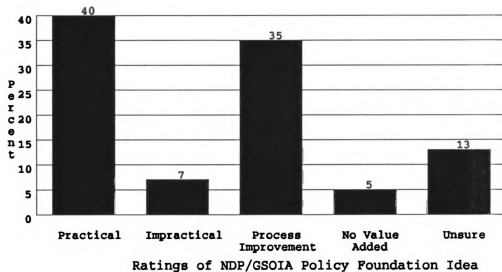
4. The prospect of key segments of defense industries coming under FOCI is the focus of debates about increased foreign investment. Hawks cite security issues to back protectionist views while doves support investment to reduce U.S. economic woes. Non-partisans tell policymakers to exercise caution for too many restrictions could be detrimental, by sparking retaliation against U.S. investment abroad and by forcing the Government to help some failing firms. Alliances could be disrupted when declining defense budgets make cost-sharing among countries more attractive. The objective is to prudently regulate, yet endorse international economic cooperation.

Improved FOCI adjudication must start with a sound policy foundation that addresses the political aspects of this issue, especially access to the "proscribed" classifications of TOP SECRET, COMSEC, Restricted Data, Special Access Programs, and Sensitive Compartmented Information. Thus, one process improvement idea is to convince all parties, foreign and domestic, government and industry, that the foundation exists in the U.S. National Disclosure Policy (NDP) and General Security of Information Agreements (GSOIA) with friendly foreign nations. The GSOIA set standards for

safeguarding classified material and the NDP regulates release of classified defense technology and articles to foreign governments through a Committee chaired by the DoD with membership from Defense, State, the Services, the Joint Staff, and other special members. The Committee maintains Delegation Disclosure Letters (DDL) for each nation specifying levels of generally releasable classified information, and the specifics of programs like foreign military weapons sales. If an "exception to NDP" is requested, an "expression of interest" must be filed by the foreign country. A NDP Committee member must "sponsor" the exception, draft justification and staff it for review. Rationale from the foreign government or U.S. mission in that country must convince the sponsor that an exception is in the national interest, isn't precluded by law or treaty, and benefits the DoD and the sponsor. A sponsor may come from outside the DoD, depending on the program (e.g., nuclear or intelligence issues). Most exceptions are approved, with denials stemming from conflicting national policies or treaty obligations, inhibiting laws, insufficient justification, or lack of a GSOIA. All NDP exception votes must be unanimous.

Political battles could be avoided and process improvements realized, if the NDP/GSOIA framework is applied to the National Interest Determination (NID) in FOCI adjudication. For instance, if the NDP/GSOIA allow release of COMSEC to Canada, but not Japan, an equitable policy premise supports limits on access by firms with FOCI stemming from that

nation. If NDP/GSOIA revisions result from changing world politics, or an exception to NDP is granted after a government files an expression of interest in support of an investor; access limits, threat, risk, and countermeasures can be reassessed in affected firms. Risks can be gauged by; a) the NDP, b) the GSOIA, and c) personnel clearance criteria. The responsibility of cleared citizens with, or without FOCI, is afterall the same. What is your opinion? Select all that apply.



		PRACTICALITY		Row Total
		Practical	Impractical	
EMPLOYMENT	Non-FOCI Firm	30	5	35 70.0%
	FOCI Firm	13	2	15 30.0%
	Column Total	43 86.0%	7 14.0%	n=50 100%

$$\chi^2(1) = .007 \quad P = .93$$

		VALUE		Row Total
		Process Improvement	No Value Added	
EMPLOYMENT	Non-FOCI Firm	24	3	27 64.3%
	FOCI Firm	13	2	15 35.7%
	Column Total	37 88.1%	5 11.9%	n=42 100%

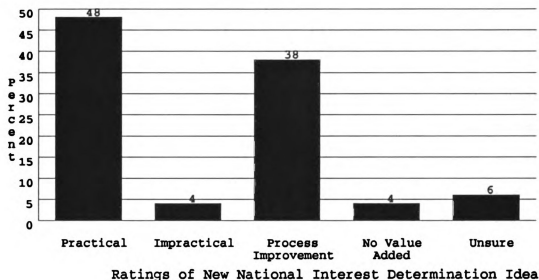
$$\chi^2(1) = .045 \quad P = .83$$

Figure 3.12 Ratings of the
National Disclosure Policy/General Security
of Information Agreement FOCI Policy Foundation Idea

Survey question 5 addressed the idea of creating a new, threat focused, three step National Interest Determination process.

5. A National Interest Determination (NID), is a pre-requisite to "proscribed" information access in a FOCI firm with a Special Security Agreement (SSA). The DoD defines a NID as an essential, impending, or prospective need to use, on a classified basis, the products, services, or technical expertise of a U.S. firm under FOCI when cleared or clearable firms are unavailable or insufficient to satisfy industrial preparedness, mobilization, planning research, production, or production base requirements of a DoD component or a participating non-DoD agency.

Spearheaded by acquisition versus security disciplines, critics of the NID process view it as costly, inefficient and misdirected. Rather than defining security solutions to counter threats to classified material, the NID reaffirms procurement needs and source selections. Schedules are impacted and competition stifled while the NID is characterized as a process of "passing the buck" for acceptance of FOCI risk from the procurement official to the component's Assistant Secretary. Given the premise in number 4 above, where proscribed access would be defined by the NDP/GSOIA, how would you rate the idea of altering the NID to three steps; 1) an intelligence and technology assessment, 2) a threat measurement and risk analysis, 3) security counter-measures planning? Select all that apply.



PRACTICALITY

EMPLOYMENT	PRACTICALITY		Row Total
	Practical	Impractical	
	Non-FOCI Firm	FOCI Firm	
	29	3	32
	23	2	25
	Column Total	5	n=57
	91.2%	8.8%	100%

$$X^2(1) = .03 \quad P = .85$$

VALUE

EMPLOYMENT	VALUE		Row Total
	Process Improvement	No Value Added	
	Non-FOCI Firm	FOCI Firm	
	25	2	27
	16	3	19
	Column Total	5	n=46
	89.1%	10.9%	100%

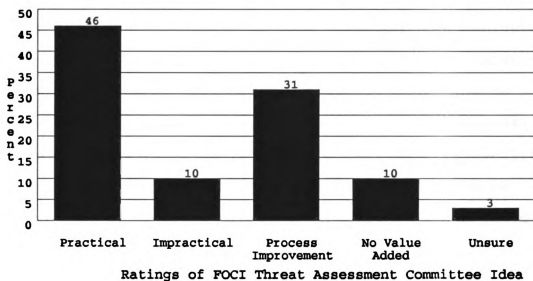
$$X^2(1) = .8 \quad P = .36$$

Figure 3.13 Ratings of the New, 3 Step, NID Process Idea

Questions 6 - 7 addressed the intelligence ideas of a Threat Assessment Committee and an automated NISP Form 441S.

6. In the 1993 Defense Authorization Conference, Congress generated legislation addressing the first two steps in question 5 by requiring a database on contract awards over \$100,000 to FOCI firms, an annual report analyzing defense critical technology contracts, and a risk assessment on any pending or proposed merger, acquisition or takeover of a U.S. firm in a defense critical technology area by a FOCI entity. This legislation affirmed the need for valid, reliable intelligence in FOCI adjudication. In parallel, the NISP initiative seeks a single, coherent, and integrated Executive Branch strategy to safeguard national security information, including standardized FOCI adjudication.

As the Intelligence Community is reorganized to address post Cold War issues, the traditional split of responsibility along foreign (e.g., CIA) and domestic (e.g., FBI) lines may not be successful. FOCI adjudication, for instance, will require a comprehensive report dealing with the ability of the U.S. operations of a FOCI firm to safeguard classified material, as well as any threats posed by the foreign parent or government. This concept of an intelligence product describing threat associated with an entire corporate lineage suggests an integrated foreign and domestic intelligence apparatus is required. How would you rate the idea of establishing an interagency NISP FOCI Threat Assessment Committee? Select all that apply.



		PRACTICALITY		Row Total
		Practical	Impractical	
EMPLOYMENT	Non-FOCI Firm	29	6	35 62.5%
	FOCI Firm	17	4	21 37.5%
Column Total		46 82.1%	10 17.9%	n=56 100%

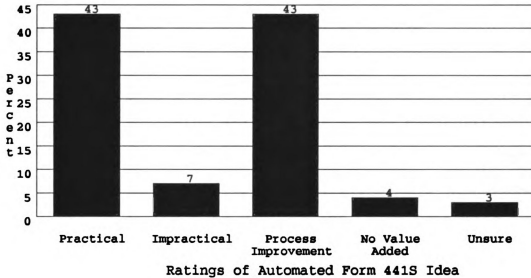
$$X^2(1) = .03 \quad P = .85$$

		VALUE		Row Total
		Process Improvement	No Value Added	
EMPLOYMENT	Non-FOCI Firm	21	6	27 65.9%
	FOCI Firm	10	4	14 34.1%
Column Total		31 75.6%	10 24.4%	n=41 100%

$$X^2(1) = .20 \quad P = .65$$

Figure 3.14 Ratings of the FOCI Threat Assessment Committee Idea

7. The Form 441S "Certificate Pertaining to Foreign Interests" is the primary FOCI data collection tool. Its effectiveness has been challenged as some questions are ambiguous and information is updated infrequently. In global markets, relations with banks, customers, suppliers, etc., change rapidly, which affects 441S accuracy. Recognizing the 441S submittal is sensitive, to improve the currency, reliability and validity of the legislatively mandated FOCI database while protecting industry proprietary interests, how would you rate the concept of automating the NISP Form 441S in a secure distributive processing network? Conceptualize a new government furnished, menu driven, database management software survey questionnaire for cleared contractors. It would provide "help" screens to eliminate question ambiguity and improve answer consistency. Utilization of a database management software platform would enhance Intelligence Community capabilities to rapidly integrate information fields for analysis to spot national security significant FOCI trends. Access could be limited by Contractor and Government Entity code, Facility Security Officer user identification password, software security, and perhaps encryption. Direct input by FSOs would minimize government labor costs while providing industry a method to monitor data accuracy and integrity. Successful ventures like the DISCO electronic Personnel Security Questionnaire and U.S. Visits System for international visit authorization requests could serve as models for this network. Select all that apply.



		PRACTICALITY		Row Total
		Practical	Impractical	
E M P L O Y M E N T	Non-FOCI Firm	28	6	34 60.7%
	FOCI Firm	20	2	22 39.3%
Column Total		48 85.7%	8 14.3%	n=56 100%
$X^2(1) = .79 \quad P = .37$				

		VALUE		Row Total
		Process Improvement	No Value Added	
E M P L O Y M E N T	Non-FOCI Firm	28	2	30 57.7%
	FOCI Firm	20	2	22 42.3%
Column Total		48 92.3%	4 7.7%	n=52 100%
$X^2(1) = .105 \quad P = .74$				

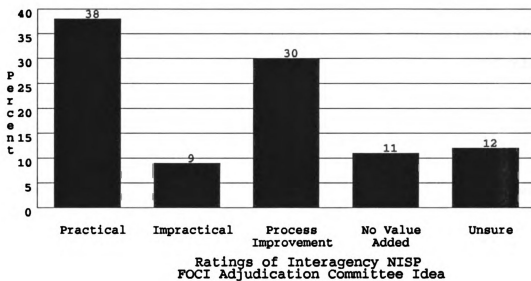
Figure 3.15 Ratings of the Automated Form 441S
"Certificate Pertaining to Foreign Interests" Idea

Survey question 8 addressed the idea of creating an interagency FOCI Adjudication Committee within the existing National Disclosure Policy Committee structure.

8. Given the National Disclosure Policy/General Security of Information Agreement policy premise for "proscribed" data access in question number 4, and improved intelligence in questions number 6 and 7, how would you rate the concept of creating an interagency FOCI Adjudication Committee by:

- a) expanding the National Disclosure Policy Committee charter to include FOCI, or;
- b) forming a FOCI Adjudication Subcommittee of the National Disclosure Policy Committee?

Select all that apply.



		PRACTICALITY		Row Total
		Practical	Impractical	
E M P L O Y M E N T	Non-FOCI Firm	27	6	33 66.0%
	FOCI Firm	14	3	17 34.0%
Column Total		41 82.0%	9 18.0%	n=50 100%

$$X^2(1) = .002 \quad P = .96$$

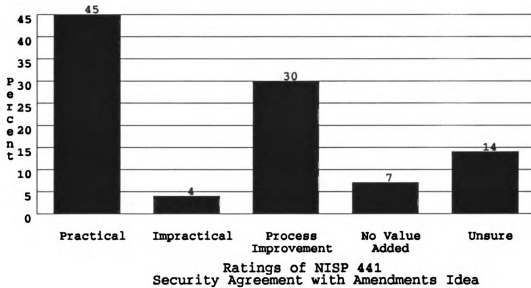
		VALUE		Row Total
		Process Improvement	No Value Added	
E M P L O Y M E N T	Non-FOCI Firm	17	7	24 54.5%
	FOCI Firm	15	5	20 45.5%
Column Total		32 72.7%	12 27.3%	n=44 100%

$$X^2(1) = .095 \quad P = .75$$

Figure 3.16 Ratings of the NISP
FOCI Adjudication Committee Idea

Survey questions 9 - 10 addressed two security countermeasures ideas. The first idea (question 9) suggested replacement of the current FOCI risk mitigation instrument terminology with a NISP Form 441 with amendments. The second idea (question 10) suggested supplemental safeguards for proscribed information in FOCI firms.

9. Despite a variety of security countermeasures options, FOCI adjudication is often reduced to either a Voting Trust/Proxy, or a SSA. Myths about the effectiveness of these alternatives then dominate ensuing debates. Unfortunately, the needs of government, the cleared firm, and the foreign investor do not always coincide with these alternatives. To define threat-driven solutions, how would you rate the idea of deleting the terms Voting Trust, Proxy, Reciprocal, Board Resolution, and SSA? Instead, the NDP FOCI Adjudication Committee (with a report from the FOCI Threat Assessment Committee) would define required countermeasure amendments to a standard NISP 441 "Security Agreement" from a list provided in the NISP Operating Manual Supplement. Select all that apply.



		PRACTICALITY		Row Total
		Practical	Impractical	
E M P L O Y M E N T	Non-FOCI Firm	28	2	30 61.2%
	FOCI Firm	17	2	19 38.8%
Column Total		45 91.8%	4 8.2%	n=49 100%
$X^2(1) = .23 \quad P = .63$				

		VALUE		Row Total
		Process Improvement	No Value Added	
E M P L O Y M E N T	Non-FOCI Firm	19	5	24 64.9%
	FOCI Firm	11	2	13 35.1%
Column Total		30 81.1%	7 18.9%	n=37 100%
$X^2(1) = .16 \quad P = .68$				

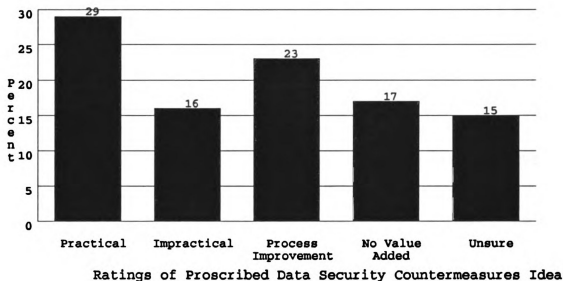
Figure 3.17 Ratings of the NISP 441 Security Agreement with FOCI Amendments versus Voting Trust/Proxy/SSA Idea

10. Given the National Disclosure Policy/General Security of Information Agreement policy premise established in question number 4 for "proscribed" information access, how would you rate the idea of providing a menu of additional safeguarding options for such data in the National Industrial Security Program Operating Manual Supplement?

For example;

- a) a Single Scope Background Investigation, normally done for TOP SECRET/Sensitive Compartmented Information, on FOCI firm employees accessing Restricted Data or Communications Security (COMSEC),
- b) a billet system to limit access,
- c) vault storage of all proscribed data.

Select all that apply.



		PRACTICALITY		
		Practical	Impractical	Row Total
EMPLOYMENT	Non-FOCI Firm	16	9	25 59.5%
	FOCI Firm	11	6	17 40.5%
Column Total		27 64.3%	15 35.7%	n=42 100%

$$\chi^2(1) = .002 \quad P = .96$$

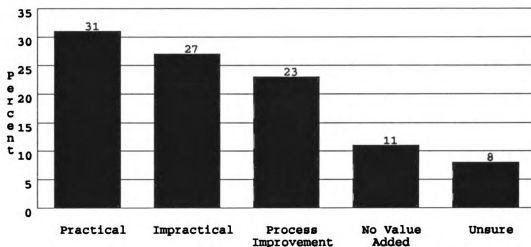
		VALUE		
		Process Improvement	No Value Added	Row Total
EMPLOYMENT	Non-FOCI Firm	10	11	21 56.8%
	FOCI Firm	11	5	16 43.2%
Column Total		21 56.8%	16 43.2%	n=37 100%

$$\chi^2(1) = 1.65 \quad P = .19$$

Figure 3.18 Ratings of the Proscribed Data Security Countermeasures Idea

Survey question 11 addressed the personnel security enhancement of ideas of a security assurance, Limited Access Authorization, and SF 312 Non-Disclosure Agreement on foreign directors in FOCI firms.

11. As a process improvement in the area of personnel security, how would you rate the idea of requiring a SECRET security assurance from the nation where FOCI stems on foreign interest Owners, Officers, Directors or Executive Personnel of FOCI firms? A Limited Access Authorization (LAA) would be granted consistent with the NDP and GSOIA for that country and they would be required to execute a SF 312 "Non-Disclosure Agreement" for prosecution under U.S. espionage laws. Select all that apply.



Ratings of Security Assurance, SF312 and LAA
for Foreign Directors Idea

		PRACTICALITY		Row Total
		Practical	Impractical	
E M P L O Y M E N T	Non-FOCI Firm	17	17	34 61.8%
	FOCI Firm	12	9	21 38.2%
Column Total		29 52.7%	26 47.3%	n=55 100%

$$X^2(1) = .26 \quad P = .60$$

		VALUE		Row Total
		Process Improvement	No Value Added	
E M P L O Y M E N T	Non-FOCI Firm	13	4	17 51.5%
	FOCI Firm	9	7	16 48.5%
Column Total		22 66.7%	11 33.3%	n=33 100%

$$X^2(1) = 1.5 \quad P = .21$$

Figure 3.19 Ratings of the Security Assurance, SF 312,
Limited Access Authorization for Foreign Directors Idea

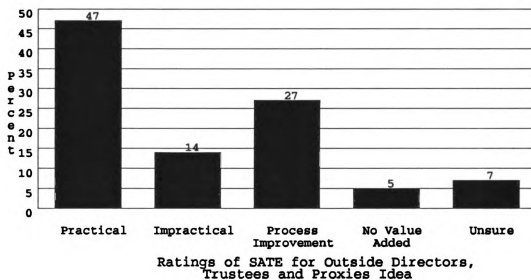
The final four questions in the survey dealt with the idea of addressing the Security Awareness, Training and Education (SATE) needs of the various groups who regularly deal with FOCI issues; Corporate Directors who perform a government watchdog role, Facility Security Officers who administer the agreements, Procurement officials who contract with the FOCI entities, and NISP Oversight and Compliance Agency officials who inspect for compliance. Since these questions are similar, they are listed together below, followed by their respective charts and cross tabs.

12. How would you rate the idea of Security Awareness, Training, and Education (SATE) to teach Outside Directors, and Proxies/Trustees both fiduciary and security responsibilities? Select all that apply.

13. How would you rate the idea of a SATE program designed to teach Facility Security Officers the key issues of FOCI? Select all that apply.

14. How would you rate the idea of a SATE program to teach Procurement agency officials the key issues of FOCI? Select all that apply.

15. How would you rate the idea of a SATE program designed to teach Industrial Security Representatives of the NISP oversight and compliance agency the key issues of FOCI? Select all that apply.



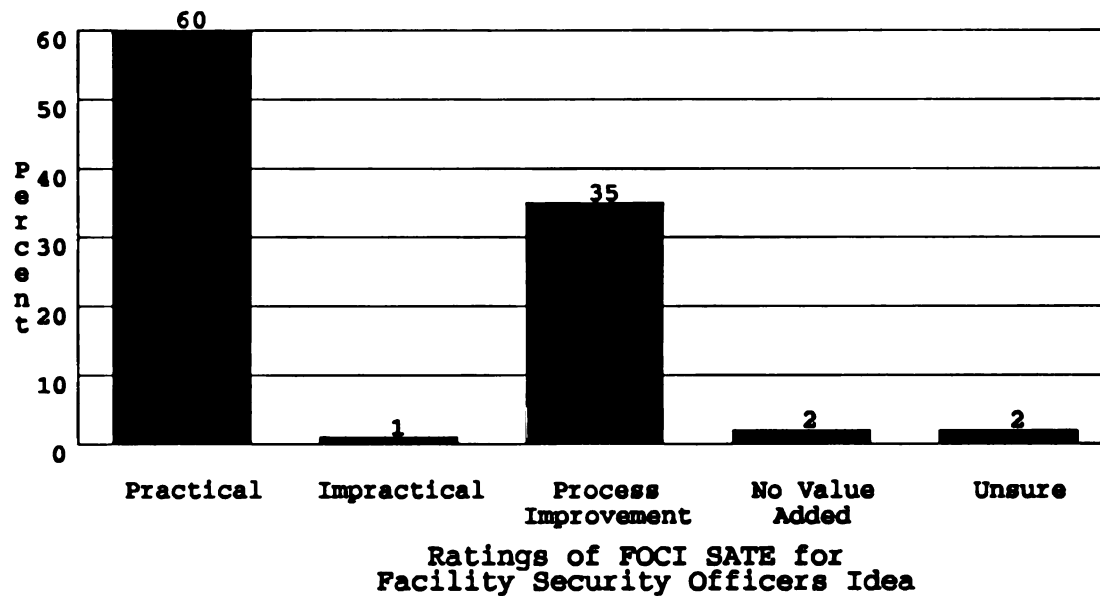
		PRACTICALITY		
		Practical	Impractical	Row Total
EMPLOYMENT	Non-FOCI Firm	29	14	43 71.7%
	FOCI Firm	17	0	17 28.3%
Column Total		46 76.7%	14 23.3%	n=60 100%

$$X^2(1) = 7.2 \quad P = .007$$

		VALUE		
		Process Improvement	No Value Added	Row Total
EMPLOYMENT	Non-FOCI Firm	15	1	16 50.0%
	FOCI Firm	12	4	16 50.0%
Column Total		27 84.4%	5 15.6%	n=32 100%

$$X^2(1) = 2.1 \quad P = .14$$

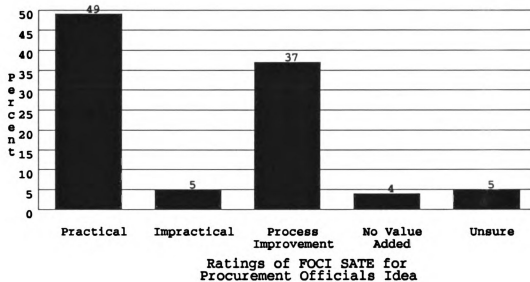
Figure 3.20 Ratings of the Security Awareness, Training and Education for Outside Directors/Proxies/Trustees Idea



		PRACTICALITY		Row Total
		Practical	Impractical	
EMPLOYMENT	Non-FOCI Firm	42	1	43 63.2%
	FOCI Firm	25	0	25 36.8%
	Column Total	67 98.5%	1 1.5%	n=68 100%
		$X^2(1) = .59 \quad P = .44$		

		VALUE		Row Total
		Process Improvement	No Value Added	
EMPLOYMENT	Non-FOCI Firm	21	2	23 56.1%
	FOCI Firm	18	0	18 43.9%
	Column Total	39 95.1%	2 4.9%	n=41 100%
		$X^2(1) = 1.64 \quad P = .19$		

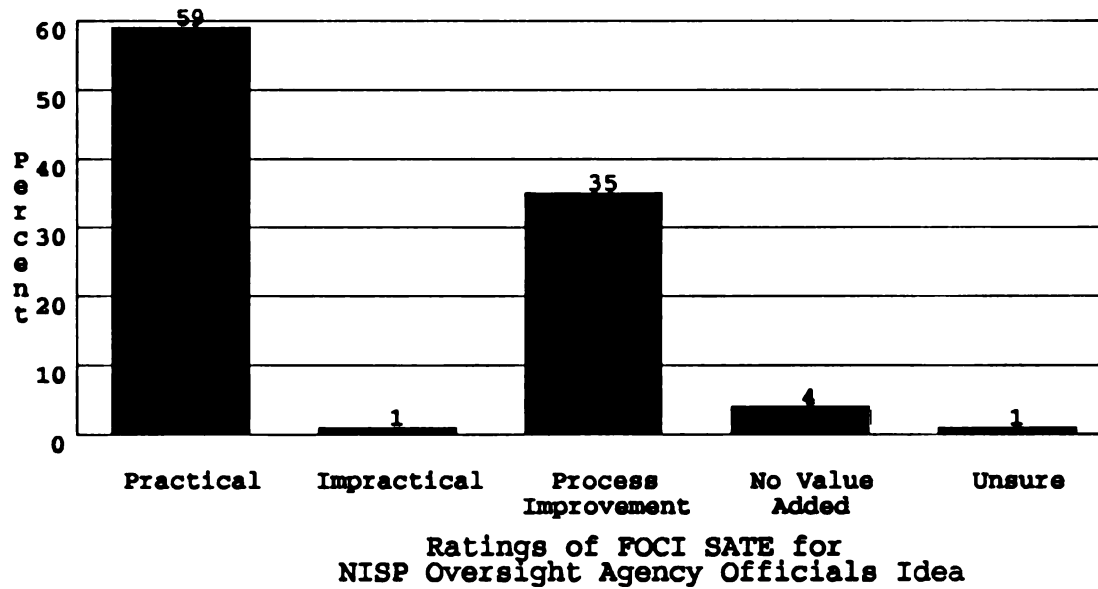
Figure 3.21 Ratings of the FOCI Security Awareness, Training and Education for Facility Security Officers Idea



		PRACTICALITY		
		Practical	Impractical	Row
E M P L O Y M E N T	Non-FOCI Firm	32	3	Total 35 63.6%
	FOCI Firm	18	2	20 36.4%
	Column Total	50 90.9%	5 9.1%	n=55 100%
		$X^2(1) = .03$		P = .85

		VALUE		
		Process Improvement	No Value Added	Row
E M P L O Y M E N T	Non-FOCI Firm	24	2	Total 26 59.1%
	FOCI Firm	16	2	18 40.9%
	Column Total	40 90.9%	4 9.1%	n=44 100%
		$X^2(1) = .15$		P = .69

Figure 3.22 Ratings of the FOCI Security Awareness, Training and Education for Procurement Agency Officials Idea



		PRACTICALITY		Row Total
		Practical	Impractical	
E M P L O Y M E N T	Non-FOCI Firm	36	1	37 61.7%
	FOCI Firm	23	0	23 38.3%
	Column Total	59 98.3%	1 1.7%	n=60 100%
$X^2(1) = .63 \quad P = .42$				

		VALUE		Row Total
		Process Improvement	No Value Added	
E M P L O Y M E N T	Non-FOCI Firm	21	2	23 59.0%
	FOCI Firm	14	2	16 41.0%
	Column Total	35 89.7%	4 10.3%	n=39 100%
$X^2(1) = .14 \quad P = .70$				

Figure 3.23 Ratings of the FOCI Security Awareness, Training and Education for NISP Oversight Agency Officials Idea

F. "Study" Step Six: Studying the Survey Results

In the "Study" phase of the PDSA model, step six of the action plan is invoked as the test results are observed. The purpose of this step is to determine if the planned changes in the process result in a smaller gap between the Voice of the Process and the Voice of the Customer. The opinions of industry security professionals on the merits of process improvement ideas developed during the PDSA exercise are used to determine if the gap between the Voice of the Customer and the Voice of the Process has decreased.

Consistent with the typically intense debate that occurs in the Legislative and Executive Branches of government when the topic of foreign ownership, control, or influence of the defense industrial base is raised, the survey of security professionals prompted many impassioned responses. Several respondents not only checked the blocks on the form, but many added substantive or rhetorical comments in the margins. A few even attached letters to further expound on their views, personal experiences, or frustrations with current FOCI security policy.

Conclusions drawn from the survey data are tempered by acknowledgement of the fact that the sample size is small, 77 responses out of 114 surveys distributed for a 67.5% response rate. The sample is, nevertheless, consistent with the PDSA methodology which suggests testing on a small scale with the customers. Additionally, it is important to recognize that the number of security professionals who regularly

deal with FOCI issues due to their employment in a FOCI firm, or if employed by a non-FOCI firm, because of contracts involving FOCI entities, is also small, but growing.

Given these cautions, analysis of the results begins with the demographic data developed in questions 1 and 2 (page 162) which address the employment of the respondents and the type of security arrangement employed to clear their firms. Not actually part of the PDSA test of process improvement ideas, these two questions were asked to facilitate analysis of data by FOCI versus non-FOCI firm respondent. While the data from question 1 indicates that nearly twice as many responses were received from non-FOCI firms (49) as were received from FOCI firms (28), the data from question 2 indicates that all types of current FOCI arrangements were represented in the response.

Question number 3 (Figures 3.7 - 3.11, pp. 164-168) was also not part of the PDSA test of process improvement ideas. It used a Likert style rating scale to measure the security professional's opinions on the effectiveness of current Voting Trust, Proxy, Reciprocal, Board Resolution, and SSA FOCI security countermeasure instruments. Rating choices included; Very Effective, Somewhat Effective, Somewhat Ineffective, Very Ineffective, and Unsure. Four observations are made about the data received on this question.

First, none of the Chi Square calculations were above the critical value of 3.84 at the 95% confidence level. This indicates the variables Employment and Effectiveness

are independent and FOCI versus non-FOCI firm orientation does not appear to bias the rating patterns of the respondents on the effectiveness of current risk mitigation instruments. Therefore, this factor is not related at all to the discussion of responses to this question.

Second, the percentage of respondents who chose Effective (Very Effective and Somewhat Effective combined) versus Ineffective (Somewhat Ineffective and Very Ineffective combined) when rating the Voting Trust, Proxy, Reciprocal, and Board Resolution is consistent; on average, 66% Effective, 34% Ineffective. This consistency is worth noting due to the fact that, on average, only 66% of the respondents rate these four instruments as effective, a majority, but not overwhelming. This observation becomes significant when the third comment below is considered.

Each ratings chart (Figures 3.7 - 3.11) shows that a substantial number of respondents (ranging from 18% to 32%) chose Unsure. This may be attributable to a lack of direct personal experience. Conversely, it may demonstrate what the General Accounting Office audits of DoD FOCI security policy have underscored, the fact that it is difficult to determine whether these arrangements really work on an operational basis, since performance criteria vary among companies. Referring back to point number two above, if the Unsure responses are viewed with the Ineffective ratings, the overall confidence level is somewhat bleak.

The fourth, somewhat surprising observation, pertains

to the SSA cross tab on page 168, Figure 3.11. In contrast to the results on the other four instruments, and despite the controversy surrounding the SSA during the GAO audit (1990, March 21) and the Thomson CSF/LTV case in 1992 (Pearlstein, Hayes, Wartzman), 51 out of 59 respondents (86.4%, which does not include those Unsure), rated the SSA either Very Effective or Somewhat Effective. Since the SSA attempts to tailor countermeasures to threat, and given the threat focus of the process improvement ideas developed using the PDSA methodology, it would be interesting to further pursue the reasons why the respondents rated the SSA more favorably than the other instruments.

The last set of observations pertain to the PDSA test of process improvement ideas, Figures 3.12 - 3.23. Once again, all the Chi Square calculations but one, did not exceed the critical value of $\chi^2(1) = 3.84$ with $P = .05$ or less. The exception is the practicality of Security Awareness, Training, and Education for Directors contained in the cross tab on page 190 which was $\chi^2(1) = 7.2$ with $P = .007$. Aside from chance, there is no readily apparent explanation for this result which is inconsistent with the others; therefore, it is not considered important.

In looking at the cumulative totals for each question, the first observation is that, with the exception of two ideas, the vast majority of the respondents rated nearly all of the FOCI security countermeasures ideas as both Practical and a Process Improvement. The bar graph charts in Figures

3.12 - 3.23, where Unsure ratings are included, display an obvious difference in the percentage of respondents who chose Practical and Process Improvement over Impractical, No Value Added, or Unsure. However, the cross tab charts which eliminate the Unsure ratings from consideration, provide an even more noticeable display of the ratings pattern of the respondents. In ten of the twelve cross tab charts, the percentage of respondents who rated the idea Practical versus Impractical ranged from 76.7% to 98.5%. Further, for those same ten ideas, the cross tab charts indicate that the percentage of respondents who chose Process Improvement versus No Value Added ranged from 72.7% to 95.1%.

There are two exceptions; 1) Figure 3.18, the idea on proscribed data security countermeasures, and, 2) Figure 3.19, the idea on a Limited Access Authorization (LAA) for foreign Directors based a Security Assurance from their own country and execution of an SF 312 Nondisclosure Agreement. On these ideas, a more even ratings split appears which may be explained by written comments received. On the proscribed data countermeasures idea, the value of a billet system was questioned. On the LAA/SF 312 idea, questions were raised on the applicability of U.S. espionage laws to foreign persons.

In summary, it does appear that the PDSA exercise has reduced the gap between the Voice of the Customer and the Voice of the Process, and provided a model for an improved FOCI security countermeasures process in the NISP.

G. "Act" Steps Seven and Eight: Conclusions,
Actions Required for the NISP, and Recycling PDSA

Recall that in the "Act" phase of the PDSA Cycle where the opportunity to improve the process materializes, there are two steps. In step seven, after studying the results of the pilot test, in this case the opinions of security professionals on the FOCI security process improvement ideas, the process is improved, or it is not, by creating a new mix of the five process resources: people, method, material, equipment, and environment. As suggested in the introduction, in this particular PDSA exercise, it will be up to government policymakers who promulgate and administer the FOCI security countermeasures process to act, or choose not to act, upon the findings presented in this paper. The flurry of activity associated with the recent high-profile Thomson CSF/LTV FOCI case, the GAO audit (1990) of DoD procedures, the DoD/CIA Joint Security Commission (1993), and the implementation deadline for Executive Order 12829 (1993) on the National Industrial Security Program seem to provide ample reasons for cognizant officials to at least consider the ideas and observations presented in this paper.

Finally, in step eight of the Deming Cycle, the PDSA exercise must start again. Assuming the appropriate authorities agree that at least some of these process improvement ideas warrant consideration, they should be field tested, preferably as Deming suggests, on a small scale. Then, the PDSA Cycle must begin again.

FOOTNOTES

FOOTNOTES

¹Assistant Secretary of Defense (Production and Logistics), October 1990, Report to Congress on the Defense Industrial Base: Critical Industries Planning states: the defense industrial base includes government and privately owned plants and equipment as well as government and private technology development efforts. The defense industrial base is both large and complex. It encompasses a network of prime weapon system manufacturers, many of whom are highly dependent on the DoD for business, and thousands of large and small subtier firms with varying proportions of commercial and military sales. The government-owned facilities are operated either by government or private sector firms. In addition to this vast array of United States industrial capability, our allies possess strong industries that support U.S. defense requirements. These industries often supply the U.S. with essential components and specific capabilities that enhance U.S. R&D and production efforts. In particular, the North American Defense Industrial Base (NADIB) represents U.S.-Canadian cooperation on industrial base issues.

²Inscription on the Smiths Industries Aerospace & Defense Systems Inc., Grand Rapids Division, Edward Bear Award for Team Excellence in Total Quality Management.

³Intelligence Community - described by Carter (1990) as the intelligence agencies which gather national security intelligence information such as the Central Intelligence Agency, National Security Agency, Defense Intelligence Agency, Federal Bureau of Investigation, Drug Enforcement Agency, and U.S. Customs.

⁴National Interest Determination definition supplied by the Office of the Secretary of Defense, Counterintelligence and Security Countermeasure, Industrial Security Programs Directorate to foreign-owned, controlled or influenced firms considered for a facility security clearance under the terms of a Special Security Agreement.

BIBLIOGRAPHY

BIBLIOGRAPHY

- Advisory. (1993, July). Administration sets up new commission to review government security. National Security Institute, Framingham, MA: 8(12), 2-3.
- Aerospace Industries Association. (1990, December). 1991 AIA Issues, Aerospace: A Global Industry. AIA Newsletter, 3, 6, p. 4.
- Aguayo, R. (1990). Dr. Deming: The American Who Taught the Japanese about Quality, New York, NY: Fireside.
- Anderson, M. C. (1992, June). Considerations affecting the future of industrial security. Defense Issues, 7(43). Washington, DC: American Forces Information Service.
- Anderson, M.C. (1992). A prudent approach to industrial security: The background and promise of the National Industrial Security Program. Viewpoints: A Periodical of the National Classification Management Society, II, 31-45.
- Alderman, C. (22 February 1990). Release of export controlled technical data to foreign-owned U.S. firms. Deputy Under Secretary of Defense (Security Policy) Memo I-90/10652.
- Arms Export Control Act, 22 U.S.C. § 2776 et seq. (1976).
- Assistant Secretary of Defense (Production and Logistics), (October 1990). Report to Congress on the Defense Industrial Base: Critical Industries Planning. Falls Church, VA: DoD Office of Industrial Base Assessment.
- Atwood, D. J., Watkins, J. D., & Webster, W. H. (1990, October 17). Report to the President on the National Industrial Security Program. Washington, DC: Department of Defense.
- Atwood, D. J., Watkins, J. D., & Kerr, R. (1991, October 18). Report to the President on the National Industrial Security Program. Washington, DC: Department of Defense.

- Auerbach, S. (1990, February 3). President tells China to sell Seattle firm. The Washington Post.
- Bagley, J. J., Evans, M. E. (1989). Foreign traumas; an overview of foreign acquisition of U.S. defense-related companies. Journal of the National Classification Management Society, XXV, 65-74.
- Beach, Jr., C. P. (1992, June 4). Acting DoD General Counsel testimony on Exon-Florio and DoD's role in CFIUS before the Senate Subcommittee on International Finances and Monetary Policy Committee on Banking, Housing and Urban Affairs. Washington, DC: Author.
- Brandon, H. B. (1991, May 30). NISP Threat Working Group memorandum to the NISP FOCI Working Group: Foreign Ownership Control or Influence (FOCI) Threat Assessment. Washington, DC: Author.
- Bremner, B., Payne, S., & Levine, J. B. (1992, July 20). They don't let just anyone buy a defense contractor. Business Week, p. 41-42.
- Burgess, J. (1991, March 22). Reversal of firm's sale revives national security debate. The Washington Post, p. 1.
- Burgess, J., Richards, E. (1990, October 23). Does foreign investment in U.S. pose a threat?; Japanese firms's bid for chip supplier sparks debate. The Washington Post, p. 1.
- Bush, G. H. (1992, January 29). Memorandum from the President to Secretary of Defense on the National Industrial Security Program. Washington, DC: The White House.
- Bush, G. H. (1990, December 6). Memorandum from the President to Secretary of Defense on the National Industrial Security Program. Washington, DC: The White House.
- Bush, G. H. (1992, February 3). Letter to the industrial security community on the National Industrial Security Program. Washington, DC: The White House.
- Carlucci, F. C. (1992, June 8). Acquisition of LTV by Thomson/Carlyle a win-win opportunity for all parties. Aviation Week & Space Technology, pp. 66-67.

- Carter, D. L. (1990). Law enforcement intelligence operations: concepts, issues, and terms. (Monograph). East Lansing: Michigan State University, School of Criminal Justice. (pp. 7-8).
- Chaisson, K. (1992, July 31). Thomson-CSF bails out of LTV deal. World Aerospace Weekly, Issue 578, p. 15.
- Classified Information Nondisclosure Agreement, National Security Information - Standard Forms § 2003.20, 32 C.F.R. 53 (Sept. 29, 1988).
- Clayton Act of 1982, 15 U.S.C. § 7 (1982).
- Cohen, V. D. (1989, November). Exon-Florio an imperfect tool for protecting U.S. technology. Aviation Week & Space Technology, pp. 68-69.
- Criscuoli, E. J. (July 1988). The time has come to acknowledge security as a profession. The Annals of the American Academy of Political and Social Science, 498, 98-107.
- Cunningham, W. C., Taylor, T. H. (1985). The Hallcrest report: Private security and police in America. Portland, OR: Chancellor Press.
- Defense Forecasts Inc. (1992). Foreign Investment in the U.S. Defense Industrial Base: A Sound National Strategy for America's Future. Washington, DC: Author.
- Defense Policy Advisory Committee on Trade (1990). Year-end review 1989: Report to the Secretary of Defense and the U.S. Trade Representative. Washington, DC: Author.
- Deming, W. E. (1986). Out of Crisis, Cambridge, MA: Massachusetts Institute of Technology.
- Deming, W. E. (1982). Quality, Productivity, and Competitive Position, Cambridge, MA: Massachusetts Institute of Technology.
- Diamond, J. (1991, February 20). Security. The Associated Press.
- Department of Defense, Directive 5220.22-M (January 1991). Industrial Security Manual for Safeguarding Classified Information, § 2-400 through 2-406.
- Department of Defense, Directive 5220.22-R (December 1985). Industrial Security Regulation, § 2-200 through 2-208.

- Department of Defense, Security Review Commission
(November 1985). Keeping the Nation's Secrets: A report to the Secretary of Defense on Security Policies and Practices. Washington DC: Author.
- Domestic and Foreign Investment Improved Disclosure Act of 1977, 15 U.S.C. §§ 78m, 78o (1982).
- Eastin, K. E. (1990, September). Acquisitions of U.S. defense contractors by foreign entities. US News and Analysis, 2, pp. 11-17.
- Engardio, P., Einhorn, B., & Ellis, J. E. (1992, March 9) McDonnell Douglas far east hopes are dimming. Business Week, p. 49.
- Espionage and Sabotage Acts of 1954, 18 U.S.C. §§ 793, 794, 798, 1001, 2151 - 2157.
- Executive Order No. 10865, 3 C.F.R. 398 Safeguarding Classified Information Within Industry, (February 20, 1960).
- Executive Order No. 11858, 3A C.F.R. 990 Committee on Foreign Investment in the United States, (1975).
- Executive Order No. 12356, 3 C.F.R. 66 (1982 Comp.); 47 Fed. Reg. 14874 . Safeguarding Classified Information Within Industry, (April 2, 1982).
- Executive Order No. 12829, 5 C.F.R. 58 National Industrial Security Program, (January 6, 1993).
- Export Administration Act (as amended), P.L. 96-72. (1985).
- Export Administration Regulation (EAR), 15 C.F.R. § 368.1-399.2 (1987).
- Federal Trade Commission Act of the Defense Production Act of 1950, 15 U.S.C. § 45. (1950).
- Finnegan, P. (1992, October 5-11) Congress may curb foreign buyers. Defense News, pp. 1, 42.
- Fields, J. E. (1988, April). DoD tracks foreign interest in U.S. companies. National Security Institute's Advisory, 11.
- Fields, J. E., Muscat, D. J. (1991, April 16). NISP FOCI Working Group memorandum to the NISP Threat Working Group: Foreign Ownership, Control or Influence Threat Assessment. Washington, DC: Authors.

Gallati, R. R. J. (1983). Introduction to Private Security, Englewood Cliffs, NJ: Prentice-Hall.

General Accounting Office. (1992, June 4). Foreign investment: analyzing national security related investments under the Exon-Florio provision. Testimony before the Subcommittee on International Finance and Monetary Policy, Committee on Banking, Housing and Urban Affairs, U.S. Senate. Washington, DC: Author.

General Accounting Office. (1990, March 21). Special Security Agreements permit foreign-owned firms to perform classified defense contracts: Statement for the record, GAO National Security and International Affairs Division, to the Committee on Armed Services, House of Representatives. Washington, DC: Author.

General Accounting Office (1990, March). President's decision to order a Chinese company's divestiture of a recently acquired U.S. aircraft parts manufacturer. GAO testimony before the Subcommittee on Commerce, Consumer Protection and Competitiveness; House Committee on Energy and Commerce; House of Representatives. GAO/T-NSIAD-90-21.

General Accounting Office. (1990, March). Foreign investment: analyzing national security concerns. (GAO/NSIAD 90-94).

General Accounting Office. (1990, June). Foreign investment: analyzing national security concerns. (GAO/NSIAD 90-94).

General Accounting Office. (1990, October). Foreign investment: Federal Data Collection on Foreign Investment in the United States. GAO/NSIAD-90-25BR.

Green, G. (1981). Introduction to Security, Woburn, MA: Butterworth.

Hanson, M. L. (1989). The regulation of foreign direct investment in the U.S. defense industry. Northwestern Journal of International Law and Business, 9, 658-684.

Hart-Scott-Rodino Antitrust Improvements Act of 1976, 15 U.S.C. § 18a (1982).

Hayes, A. S. (1992, April 6). Thomson's bid on LTV stirs concern about foreign control of defense firms. Wall Street Journal, A4.

Healy, R. J.; Dr. Walsh, T. J. (1971). Industrial Security Management: A Cost-Effective Approach, United States: American Management Association.

- Hicks, D. A. (October 1990). Foreign Ownership of Defense Firms Boosts US Security. Armed Forces Journal International, 56, 58, 60.
- Huge, E. C. (1990). Total Quality: An Executive's Guide for the 1990s, Homewood, IL: Business One Irwin.
- Improved National Defense Control of Technology Diversions Overseas, § 2537, 10 U.S.C. § 838 (1992).
- Information Security Oversight Office. (1988, September). Classified information nondisclosure agreement standard form 312 briefing booklet, Washington, DC: Author.
- International Investment Survey Act of 1976, 22 U.S.C. §§ 3101-3108 (1982).
- International Traffic in Arms Regulation (ITAR), 22 C.F.R. § 120.1-130.17 (1993).
- Melcher, R. A., Hollifield, A. (1992, July 20). They don't let just anyone buy a defense contractor. Business Week, pp. 41-42.
- National Security Act of 1947, as amended.
- Nadler, D. A., Gerstein, M. S., Shaw, R. B., and Associates (1992). Organizational Architecture: Designs for Changing Organizations, San Francisco, CA: Jossey-Bass Inc., Publishers.
- National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations (NDP-1), Sept. 9, 1981.
- NISP FOCI Working Group. (1991, March). Charter and Objectives. Washington, DC: Author.
- Omnibus Trade and Competitiveness Act of 1988, Pub. L. No. 100-418, § 5021, 102 Stat. 1107, 1425 (1988).
- Pagliano, G. J. (1992, April 2) Foreign Investment in U.S. Defense Companies (Congressional Research Service Report 92-331 F). Washington, DC: Library of Congress.
- Pearlstein, S. (1992, April 19). Undoing a done deal: How a few days broke Marietta's grip on LTV Aerospace. Washington Post, p. h01.
- Purpura, Philip P. (1984). Security & Loss Prevention, Woburn, MA: Butterworth.

- Scherkenbach, W. W. (1991). Deming's Road to Continual Improvement, Knoxville, TN: SPC Press.
- Scherkenbach, W. W. (1991). The Deming Route to Quality and Productivity: Roadmaps and Roadblocks, Washington, DC: CeePress.
- Securities Act of 1933, 15 U.S.C. §§ 77a-77bbbb (1982).
- Securities and Exchange Act of 1934, 15 U.S.C. §§ 78a-78kk (1982).
- Seymour, P. (1993, February 5). U.S. National Disclosure Policy. Defense Trade Controls Bulletin - Special Edition, Washington, DC: Author.
- Sherman Act of 1982, 15 U.S.C. §§ 1,2 (1982).
- Sherman, S. (1992, September 21). Are strategic alliances working? Fortune, pp. 77-78.
- Silverberg, D. (1992, October 19-25). U.S. Air Force official raps DoD's foreign investment rule. Defense News, p. 42.
- Silverberg, D. (1992, August 17-23). LTV sale fallout likely will spark process overhaul. Defense News, p. 26.
- Silverberg, D. (1992, September 21-27). DoD eyes restrictions on foreign ownership. Defense News, p. 1, 36.
- Stewart, N. J. (1992, August 28) Pentagon draft memorandum for distribution: Interim guidance on foreign ownership, control or influence (FOCI) cases. DASD(CI&SCM).
- Stewart, N. J. (1992, October 26-November 1) Commentary Letter: Mistaken Viewpoint. Defense News, p. 18.
- Suto, E. J. (1992, November-December) DIS achievement report. CM Bulletin of the National Classification Management Society Inc., XXVI(6) P. 3.
- Swim, L. (1991, October 31). [NISP FOCI Database: telephonic interview]. Defense Intelligence Agency, Washington, DC: Author.
- Thompson, T. J., Dyer, J. J. (October 1990). Foreign acquisitions of United States companies: What you don't know may hurt you. Contract Management, 18-20, 42-44, 50.

- Timm, H. W., Christian, K. E. (1991). Introduction to Private Security, Belmont, CA: Brooks/Cole.
- Tolchin, S. (1992, October 19-25). U.S. moves to guard vital industries. Defense News, pp. 27-28.
- U.S. rules on foreigner's defence sector purchases. (1991, November 20). Financial Times.
- Walton, M. (1991). Deming Management at Work, New York, NY: Peregree Books.
- Walton, M. (1986). The Deming Management Method, New York, NY: Peregree Books.
- Wartzman, R. (1992, November 2). Keep out: Foreign moves to by U.S. defense firms face higher hurdles. Wall Street Journal, pp. 1, 4.
- Wartzman, R. (1990, March 20). Japanese equity role in Boeing project grows increasingly remote, sources say. Wall Street Journal, p. 3.
- Wartzman, R. (1991, November 15) A McDonnell deal in Asia would jolt the airliner industry. Wall Street Journal, p. 1.
- Wethington, O. L., (1991, November 15). Exon-Florio Regulations - Final Rule. (Report 91-307-A). Washington, DC: U.S. Department of the Treasury.
- White House, (1993, May 26). Vice President praises effort to streamline security procedures; plan reflects goals of National Performance Review. Washington, DC: Office of the Vice President, Press Release.
- Yancey, M. (1991, June 12). Foreign Investment. The Associated Press.

MICHIGAN STATE UNIV. LIBRARIES



31293010336729