U.S. DEPARTMENT OF COMMERCE
National Technical Information Service

PB-262 195

The White-Collar Challenge to Nuclear Safeguards

Battelle Human Affairs Research Centers, Seattle

Prepared for

Nuclear Regulatory Commission, Washington, D C

Jan 77

NUREG-0156

THE WHITE-COLLAR CHALLENGE TO NUCLEAR SAFEGUARDS

Battelle Human Affairs Research Centers
for
U. S. Nuclear Regulatory Commission

BIBLIOGRAPHIC DATA SHEET	1. Report No. NUREG-0156	2.	3. Recipient's Accession No.

4. Title and Subtitle

THE WHITE-COLLAR CHALLENGE TO NUCLEAR SAFEGUARDS

5. Report Date: January 1977

6.

7. Author(s): Herbert Edelhertz and Marilyn Walsh

8. Performing Organization Rept. No.

9. Performing Organization Name and Address

Battelle Human Affairs Research Center
4000 N.E. 41st Street
Seattle, Washington 98105

10. Project/Task/Work Unit No.

11. Contract/Grant No.: NRC FIN B2092

12. Sponsoring Organization Name and Address

Division of Safeguards, Fuel Cycle and Environmental Research
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

13. Type of Report & Period Covered: Final

14.

15. Supplementary Notes

16. Abstracts

This study defines the parameters of the threat to safeguards systems posed by the white-collar adversary who uses complex schemes employing guile and deception rather than force, to attempt diversion of nuclear materials. Its aim has been to explore the potential capabilities and dangers presented by this adversary both in terms of the specific attributes of the threat he poses, and in light of the unique regulatory structure and evolutionary development of the civilian nuclear field.

17. Key Words and Document Analysis. 17a. Descriptors

Safeguards; Diversion; Special Nuclear Material; Plutonium; Uranium

17b. Identifiers/Open-Ended Terms

17c. COSATI Field Group

18. Availability Statement

19. Security Class (This Report) UNCLASSIFIED

20. Security Class (This Page) UNCLASSIFIED

21. No. of Pages

NUREG-0156
NRC-13

THE WHITE-COLLAR CHALLENGE TO NUCLEAR SAFEGUARDS

Herbert Edelhertz
Marilyn Walsh

Manuscript Completed: December 1976
Date Published: January 1977

Battelle Human Affairs Research Centers
Seattle, Washington 98105

Prepared for the U. S. Nuclear Regulatory Commission
Under Contract No. FIN B2082

1a

PREFACE AND ACKNOWLEDGEMENTS

The urgent nature of our current energy problem has compelled our society to closely examine the economic, resource, and danger potential of the civilian nuclear industry. Few aspects of this examination have been so intense as that which involves the protection of our domestic and international community against hazards arising from the possible theft of nuclear materials or their diversion to unauthorized or improper uses --- the Safeguards issue.

This study is designed to explore one of the challenges to Safeguards systems in the civilian nuclear industry, that presented by the so-called "white-collar" adversary who would employ guile and deception rather than force to achieve unauthorized objectives with respect to nuclear materials. Essential to this initial exploration has been definition of the problem, setting of its parameters, and consideration of its significance both for the regulatory responsive capability of the U.S. Nuclear Regulatory Commission and for the industry which it regulates.

This work necessarily depended upon the support, cooperation, and guidance provided to the authors by many individuals in the civilian nuclear industry, the research community, and the U.S. Nuclear Regulatory Commission. Special thanks are due to Frank Arsenault and John L. Berggren of the U.S. Nuclear Regulatory Commission for their helpful and informative monitoring of our work in progress, and to Theodore S. Sherr and William M. Murphey of the Commission and R. K. Mullen (Consultant to the Commission) who joined with them in providing us with extensive and valuable comments on the draft version of this report.

We are also grateful to Carl A. Bennett and John Hebert of the Battelle Human Affairs Research Centers whose comments and suggestions added greatly to such value as this report may have, and to Roma St. James who carefully superintended the actual production of this report, kept us to our deadlines, personally designed its layout, and prepared its illustrative tables.

Herbert Edelhertz

Marilyn Walsh

TABLE OF CONTENTS

TABLE OF CONTENTS (continued)

ABSTRACT

This study defines the parameters of the threat to safeguards systems posed by the white-collar adversary who uses complex schemes employing guile and deception rather than force, to attempt diversion of nuclear materials. Its aim has been to explore the potential capabilities and dangers presented by this adversary both in terms of the specific attributes of the threat he poses, and in light of the unique regulatory structure and evolutionary development of the civilian nuclear field.

I. INTRODUCTION

Special nuclear materials have great value, whether measured in strategic or money terms. They have both symbolic and intrinsic worth. These characteristics make them attractive, albeit extraordinarily difficult targets for thieves --- the difficulty stemming primarily from the fact that levels of protection are geared to strategic and symbolic value and to safety and health considerations rather than only to intrinsic worth. Under these circumstances carefully designed Safeguards systems, supported by an extensive research program, have been and are a logical development.

Current Safeguards systems clearly take into account the danger of overt physical threats, and also that of relatively unsophisticated criminal acts on the level of conventional attempts by employees to steal their employers' property. This study defines the parameters of the threat to Safeguards systems posed by the white-collar adversary who uses complex schemes employing guile and deception rather than force, to attempt diversion of nuclear materials. Its aim has been to explore the potential capabilities and dangers presented by this adversary both in terms of the specific attributes of the threat he poses, and in light of the unique regulatory structure and evolutionary development of the civilian nuclear field. As such this study has been a search for initial description and analysis of a problem and not an attempt to make definitive adversary capability assessments or to prescribe specific problem solutions.

In this report the potential vulnerability of regulated civilian nuclear facilities to diversion or related violations is addressed against the backdrop of those practices and devices commonly referred to as "white-collar crime." The nuclear threat analogy to "white-collar crime" would be:

> *an illegal act or series of illegal acts committed by non-physical means and by concealment or guile, to steal or divert nuclear materials or to otherwise deprive the U.S. Nuclear Regulatory Commission or licensees of information necessary to achievement of Safeguards objectives.*

It is quite clear that the current system of regulation, monitoring and inspection is not blind to the dangers of diversion or related violations committed by non-physical means and by guile and deception. One can examine these current systems and come to the conclusion that the mechanisms they employ would prevent diversion or other violations committed by guile and deception, or at least ring alarms before any substantial harm results. The key question is whether these checks and redundant mechanisms can be relied on for assurance that Safeguards objectives are being achieved in the light of white-collar threats.

A. BACKGROUND AND ORIENTATION

The term "white-collar crime" has been used to describe a broad spectrum of illegal or wrongful activities which fall outside the area of common crimes such as crimes of violence and relatively crude thefts. A useful and widely accepted definition is:

> *an illegal act or series of illegal acts*[1] *committed by non-physical means and by concealment or guile, to obtain money or property, to avoid the payment or loss of money or property, or to obtain business or personal advantage.*[2]

This definition has achieved substantial acceptance, principally because it addresses the nature and character of the wrongful activity involved rather than the social or economic status of the offender.[3]

It is important in considering the issue of white-collar crime, whether in the nuclear industry or more generally, that the scope of activity being considered not be limited by the narrow parameters of criminal violations. The very same activity may well be treated as a criminal violation, the basis for a civil claim, or as a basis for some administrative action.[4] For example, in a government procurement matter where there is doubt about the deliberateness of a false claim or insufficient quantum of proof, the remedy invoked might be a contract termination rather than criminal prosecution.[5] If we are concerned about threats from white-collar type crimes in the nuclear area, the scope of

---

[1]The term "illegal acts" is usually defined to include misrepresentations by omission or otherwise which deprives a regulatory agency of information necessary to carry out its responsibilities. See pp. III-2 & V-5 infra, and 18 U.S.C. 1001.

[2]Herbert Edelhertz, The Nature, Impact and Prosecution of White-Collar Crime, U.S. Department of Justice, L.E.A.A., (U.S. Government Printing Office, 1970), p. 3. This definition was described as a "good working definition" in the Attorney General's First Annual Report on Federal Law Enforcement and Criminal Justice System Assistance Activities (Washington, D.C.: U.S. Government Printing Office, 1972, p. 161).

[3]See Walter C. Reckless, The Crime Problem (4th Ed., New York: Appleton-Century-Crofts, 1973, pp. 315-333); Martin R. Haskell and Lewis Yablonsky, Criminology: Crime and Criminality (Rand McNally: Chicago, 1974), pp. 13-14, 150; Charles E. O'Hara, Fundamentals of Criminal Investigation (4th Ed., Springfield, Ill.: Charles C. Thomas, 1976, pp. 902-906).

[4]Note 2, supra, pp. 21-22.

[5]Id.

our examination should be broad enough to cover the possibility of *all* uses of deceptive measures which *could be employed* to execute diversions of or to disguise the true state of nuclear material inventories or transactions.[6]

It is also important in considering the white-collar crime threat to nuclear facilities that reliance not be placed on the infallibility of systems simply because (a) we are aware of no instances where they have been breached through devices of fraud or deceit, or (b) provision has been made for checks and balances which would "inevitably" surface breaches of the system. Well executed fraud activities may never be discovered. If they are discovered, various pressures may inhibit reports of crime from being made. Little is known about the extent to which internal audit controls deter or prevent embezzlement or insider fraud (in business or government), but we do know that such crimes are often committed in the face of the most careful checks and balances by inside financial and material controllers, independent certified public accountants retained by management, and external examiners, e.g., government auditors on public contracts. Many such crimes have defied detection for long periods of time, which has convinced white-collar crime experts and investigators that many such crimes are never discovered. Similarly, we should not assume that a protection system has the capacity to frustrate any reasonably forseeable white-collar threat scenario simply because it is very difficult to construct such a scenario; the history of white-collar crime is replete with successfully executed scenarios which would have been easy to write if hindsight were foresight.

The fact that there may be a white-collar crime threat to the integrity of nuclear Safeguards systems does not necessarily mean that special protective mechanisms or regulations beyond those now in existence or contemplated are called for. What is necessary is that the dangers to the integrity of these systems from crimes, violations, or infractions of these types be clearly delineated, that there be a clear understanding of the *modi operandi* of such schemes, and that the risks involved be given proper weight along with other more easily comprehensible threats in the design of Safeguards systems.

While overt physical threats are generally more easily conceptualized and understood, white-collar adversaries represent a different and distinct challenge. They are unlikely to be "outsiders," their motives will likely be different from other adversaries, their objectives will differ and will be apt to change over time. Most important, one high priority objective of such adversaries will be to cover up the fact that thefts have taken place, or to delay discovery for a period of time which will either make it unclear whether there have been thefts or impossible to trace the thieves.

---

[6]The danger of diversion by guile and deception has been recognized as an important Safeguards concern. See Bennett, C.A., Murphey, W.M., Sherr, T.S., Societal Risk Approach to Safeguards Design and Evaluation, USERDA Report ERDA-7 (June 1975, p. 37 et seq.)

It is useless to try to replicate the physical threat scenario in the white-collar area insofar as that scenario relies on contrasting measurements of target hardness versus numbers and equipment of adversaries. In the world of white-collar crime there are only rarely outer or inner perimeters to be physically breached; one or a few persons strategically placed will be more of a threat than a larger number. Since illegal activities must take place over a considerable period of time, fewer participants mean "fewer moving parts" to go wrong and disclose an operation.

Deceitful activities do not lend themselves to frontal assaults. They are more likely to occur where nuclear materials change custody, as between nuclear facilities or between departments or sections within plants. Attacks, then, are likely to be made at the joining points between elements of a system --- where there is just that slight uncertainty as to who is controlling the activity. Should there be a white-collar assault at such a juncture, and should it be discovered, it may be far too late to move up and respond effectively.

* * *

Regulation of the civilian nuclear industry, including current Safeguards systems, evolved in a manner quite different from that of all other regulatory systems. While this makes analogies difficult, and possibly misleading, it also operates to inhibit the transfer of regulatory techniques and experience, and may contribute to an absence of controls in the nuclear area which may be found in other regulatory areas.

Regulatory agencies or functions generally develop along an almost Toynbee-like theoretical dimension of challenge and response. First there is an industry or trade which grows over a period of time, totally unregulated. Because of the growing economic power of its units, alone or in combination, it abuses its customers or less powerful competitors. In other instances the industry's products centrally affect the health or safety of customers or the community. At first abuses affect only a small number of victims, who may be politically powerless; then more are affected. Customary legal remedies or private economic controls are inadequate, control of the industry becomes a political issue, and regulatory mechanisms are established. This pattern holds whether we look at transportation systems, public utilities, meat packers, pharmaceutical manufacturers, financial institutions, and even trades or professions.[7]

Such regulatory mechanisms are structured to meet known and well-documented threats, and responses are specifically designed to cope with what is experienced and understood.

---

[7]It should be recognized that other factors come into play in many instances, particularly where control for some public purpose becomes a vehicle for restricting entry into a trade or profession, or where regulation serves the dual purpose of setting professional standards *and* limiting competition.

As the new regulatory system is challenged by innovative attempts to circumvent its regulatory controls, revised statutes, regulations, and monitoring or inspection techniques evolve to meet such new challenges --- once again based upon the occurrence of documented events which strongly signal some gap in the regulatory agency's capability to respond to a formerly unperceived weakness or, more often, to changes over time in the nature of adversary activity or the environment in which regulatees exist and conduct their business.

A factor of great importance in this conventional regulatory situation is that the evolution of regulatory practices is carried out in the open and is subject to influence by a relatively large sector of the public --- which has specific rather than general interests. For example, personal injury lawyers focus a glaring spotlight on possible absence of safety features in automobiles, aircraft, and other products such as pharmaceuticals; stockholder losses make it more likely that insider fraud by corporate officers will be closely investigated by the U.S. Securities and Exchange Commission and by prosecutors. Relatively frequent and public events (none of which are individually so fateful and fraught with consequences for disaster, or so emotionally charged as would be diversion of critical quantities of plutonium) therefore determine the nature of conventional regulatory activity. This is hardly the case with nuclear Safeguards, or with other nuclear regulatory activity.

The private nuclear industry was created largely on the basis of experience gained in industrial contractor operations. These contractors and other private sector enterprises were permitted to use, refine, and expand on technologies developed largely in government laboratories. For a long period this process took place outside the view of the general public. Surveillance was largely the province of highly informed groups concentrated in the Atomic Energy Commission and private industry, together with a relatively small percentage of knowledgeable and interested legislators and private citizens. While the mechanisms of material accounting and physical protection were developed as an adjunct to the need for security and the inherent value of the products, it was necessary to intellectualize the development of Safeguards responses to external threats --- relying largely on models, scenarios and a small number of instructive events which could transmit clear and unequivocal messages to be used as steering mechanisms for Safeguards design and operations.

No large cadre of "outsiders," such as victims suffering personal or economic loss --- or their attorneys --- were available to make inputs to this regulatory system, especially with respect to Safeguards. Even now the main outsider inputs, developing politically, for example, in the area of reactor safety, must essentially orient themselves around issues identified by and studies commissioned by NRC and ERDA, rather than as the result of separately conceived critiques based upon events, experiences, and independent research.

This unique evolutionary development was probably inevitable. Its significance to the particular issue of vulnerability of nuclear facilities to white-collar crime type violations and abuses is that these evolutionary differences may have obscured the existence of commonalities among the challenges faced by the nuclear industry and other regulators --- with consequent failure to fully exploit experiences from outside the nuclear industry.[8]

A further result of this evolutionary development is that there is no clear way to assess the efficacy of the regulatory structure. Safeguards regulations, supplementary material such as regulatory guides, and monitoring or inspection procedures respond in most instances to purely hypothetical hazards not based on experience. This absence of a clearly demonstrable basis for determining regulatory objectives and requirements must necessarily inhibit the most conscientious regulators from what might appear to be cavalier imposition of conditions which would be costly or otherwise onerous to licensees.

B. SIGNIFICANT ISSUES

In the course of this study, the writers were struck with the existence of what can only be called a "double standard," applying one scale of values to threats by armed assailants or sneak thieves on the one hand, and an entirely different standard for white-collar adversaries. This became evident along two dimensions. First, the absence of verified diversions by physical force is seen to be no basis for lack of continued and intense attention to the threat; the lack of similar indications of diversion by guile and deceit is frequently given as a justification for failing to give similar attention to the white-collar threat.[9] Second, the absence of *some* market or purpose for stolen SNM is never advanced as a reason for not giving a high level of Safeguards attention to the threat of diversion by physical force, while the absence of a definable market for materials stolen by guile and deception is noted as one reason for a different and less urgent regulatory response to the problem of the white-collar threat. This second example may be based on the instinctive and intelligent perception that SNM stolen by guile and deception may have an entirely different market or intended use than that acquired by physical assault or common theft.[10]

---

[8]See Section V, Regulatory Comparisons, pp. V-1-7.

[9]NRC research and regulatory operations clearly reflect the agency's concern for the potential of the internal threat, of which the white-collar adversary is a part. However, there appears to be no comparable concern on the part of the civilian nuclear industry itself.

[10]See p. I-7 infra.

One reason for the differential attention given to the white-collar adversary may be the assumption that systems designed to frustrate petty theft, to protect licensees' costly property, or meet quality control or safety standards are adequate protection against white-collar diversions. This is an assumption which should be questioned.

The issue of a market for stolen nuclear materials is a central and important one, especially in the white-collar area. While much doubt has been cast upon the attractiveness of nuclear material to those who contemplate its use as an explosive or contaminant for terrorist or extortive purposes,[11] there is little question as to its intrinsic value, principally abroad and in areas not subject to international inspection. While this may now be a limited, or even non-existent market, the situation will tend to change with proliferation of nuclear facilities abroad. Developments abroad which alter patterns of demand for and legal access to nuclear materials may thus create new challenges for domestic Safeguards authorities in supplier countries such as the United States.

* * * *

There is one generally-recognized danger which merits special consideration with respect to the white-collar adversary. Safeguards monitoring and inspection may too easily become a variation of safety or quality control based upon the assumption that if licensee operations comply with prescribed tests, no diversion or other adversary act can take place. Thus compliance with regulations and procedures may erroneously become operationally synonomous with meeting Safeguards objectives. Given all these circumstances, wide swings in the intensity of regulatory controls should be anticipated in response to real or misconceived dangers. There is thus a situation most subject to regulatory "oversteering" since forward directions will rarely be clear.

* * *

Finally, a major reason for concern about the adequacy of Safeguards regulations in relation to the white-collar adversary stems from (1) prospective future increases, by orders of magnitude, in the numbers of transactions (sales or other transfer events), which may provide increased opportunities for white-collar adversary acts, and (2) lowered levels of regulatory surveillance in relationship to growth in the volume of transactions which may reasonably be anticipated. Historically, as the scope of

---

[11]Several studies point out that terrorist groups can more easily and safely acquire and use conventional destructive devices or material. Nevertheless there is a distinct possibility that such groups may have the financial ability to finance acquisition of nuclear materials diverted by covert means. Such an intersection between the white-collar and the terrorist adversary could be assisted by a market structure in which neither would be identified to the other.

a regulated industry's activity increases, budget levels to provide resources lag further and further behind --- even where frequent and regular crimes and violations are uncovered. If the nuclear industry expands along lines predicted, with numbers of transactions increasing dramatically, it is difficult to foresee any deviation from this pattern. Like other regulatory agencies, the U.S. Nuclear Regulatory Commission will have to develop innovative and imaginative regulatory techniques to cope with this challenge --- at which time utilization of other regulatory experience in the white-collar crime area should be not only valuable but absolutely essential.

* * *

In sum, when considering the white-collar adversary threat to nuclear Safeguards systems, the following points should be kept in mind:

- the absence of current information about white-collar acts against nuclear Safeguards systems does not justify the conclusion that no such acts have taken place, that they are unlikely, or that current Safeguards systems are prepared to deal with them;

- the fact that there may be a credible white-collar adversary threat to nuclear Safeguards systems does not necessarily imply that elaborate or extensive mechanisms or changes in regulations are required to deal with this threat;

- the unique evolutionary development of regulation of the civilian nuclear industry may have significant implications for Safeguards responses to the threat posed by the white-collar adversary;

- the lack of comprehensive and systematic attention to the white-collar adversary may in fact represent a significant gap in the comprehensiveness of Safeguards systems;

- the achievement of nuclear Safeguards objectives with respect to the white-collar adversary may not be assured by achieving compliance with existing Safeguards procedures; and

- the threat presented by the white-collar adversary may be expected to grow with the domestic and international expansion of the civilian nuclear industry.

II. THE APPROACH TAKEN IN THIS STUDY

This study is grounded upon a general overview of nuclear Safeguards systems and the industrial and regulatory environment in which they operate --- from a perspective of familiarity with white-collar crime activity and regulatory measures to deter, detect, investigate, and prosecute such activity. It is designed to apply a body of knowledge from another area to the nuclear regulatory area, and it will therefore possibly overlook many points which would be readily apparent to those engaged in on-going nuclear regulatory activity, specialized research in the nuclear field, or licensee operations.

In this study relatively little emphasis is placed upon the particular text of current regulations or supplementary material. An examination of potential Safeguards vulnerabilities confined within the parameters of and focused upon existing regulatory textual and operational material would initially have involved a parsing of papers and procedures rather than priority consideration of the risks and hazards to which they respond. More is to be gained, at this juncture, by looking at the nature of vulnerabilities.

The following portion of this report therefore begins with a general discussion of the character and elements of white-collar crime. The purpose of this discussion is two-fold. First, it orients the reader to the background and ramifications of the definition of nuclear white-collar crime used in this study:

> *an illegal act or series of illegal acts committed by non-physical means and by concealment or guile, to steal or divert nuclear materials or to otherwise deprive the U.S. Nuclear Regulatory Commission or licensees of information necessary to achievement of Safeguards objectives.*

Second, this discussion of white-collar crime based on consideration of its elements, makes it possible for those with more specific knowledge of the nuclear field to read their own expertise and experience into this work, and to draw their own conclusions and make their own recommendations --- as a supplement or in contradiction to the comments and conclusions contained in this report.

From definition of the problem, this report then examines possible hazards and threats presented by the white-collar adversary. Its consideration of relevant adversary characteristics, adversary motives, and the ways in which this adversary may operate is intended to round out the full range of adversary threats presently facing Safeguards enforcement efforts. It is not meant to imply that such adversaries are currently operating in the manner we describe.

Based on the foregoing, and on a review of the regulatory environment and challenge, we conclude that white-collar crime and related abuses are a credible threat. Further, we speculate that while an increase across the full spectrum of possible threats of theft or diversion of nuclear materials is to be expected because of projected expansion of domestic and international commercial trade in such materials, the white-collar adversary will become more significant relative to other adversaries.

III. THE CHARACTER AND ELEMENTS OF WHITE-COLLAR CRIME

It is possible to examine white-collar crimes along three dimensions. The first is to consider the elements of the crimes, to determine what crimes satisfy the general (non-Safeguards) definition of a "white-collar" crime as:

> . . . *an illegal act or series of illegal acts committed by non-physical means and by concealment or guile, to obtain money or property, to avoid the payment or loss of money or property, or to obtain business or personal advantage.*[12]

The second is to consider a division or categorization along the lines of offender types, motivations, or the environment in which such violations are committed. A third approach might be a categorization based on the nature of the victim, e.g., a government, business entity, or individual.

For the purposes of this report we will consider white-collar crimes along the first of these dimensions, which has heretofore been considered most relevant for law enforcement purposes[13] and as a basis for criminological analysis.[14] NRC's mission in the Safeguards area is, after all, essentially a law enforcement mission.

There are five principal elements in a white-collar crime or related abuse. They are:

1. Intent to commit a wrongful act or to achieve a purpose inconsistent with law or public policy;
2. Disguise (of purpose);
3. Reliance by adversary on ignorance or carelessness of victim;
4. Voluntary victim action to assist the adversary; and
5. Concealment of the violation.

Each of these elements is defined and discussed below.

---

[12]Edelhertz, op. cit., Note 2.

[13]Notes 2 and 3, op. cit.

[14]Note 3, op. cit.

1. Intent to Commit a Wrongful Act or to Achieve a Purpose Inconsistent with Law or Public Policy

The application of this element in the context of Safeguards should not be confined to acts which are technically criminal since the regulatory objective must be to deter, prevent, detect, and take action, regardless of whether or not an offense is capable of being proved beyond a reasonable doubt, which is the criminal standard of proof. It should be enough, in this context, that there be a *deliberate* involvement in diversion, or some act *calculated* to deprive a nuclear facility or NRC of the opportunity to (a) learn of a possible diversion, (b) infer that there are circumstances which might indicate the possibility of a diversion, (c) discover that nuclear materials are missing, (d) find out that protective facilities or devices are not constructed or operating pursuant to Safeguard specifications or license conditions, or (e) learn that the integrity of NRC-mandated record keeping or reporting requirements are being distorted or manipulated in a manner which would limit or detract from the ability of NRC or the licensee to know facts which might indicate a diversion if such data would surface in the absence of such distortion or manipulation.

These criteria should be broadly interpreted, in a manner parallel to that of the legal doctrine of "materiality," which turns on the question whether the Federal Government would have been in a position to consider taking action except for a failure to properly comply with a record keeping or reporting requirement.

In the non-nuclear regulatory context it is well settled that white-collar crimes and related abuses may be committed by acts of omission as well as commission. For example, it has clearly been held that failure to register a security issue with the U.S. Securities and Exchange Commission is tantamount to fraud because it serves to deny the investing public the protections of full disclosure required by the Securities Act of 1933. Our courts have recognized that fraud may well be the motivation for violation of these so-called registration requirements. Such frauds may be subject to either criminal or civil penalties; a showing that the making of registration statement would not have shown facts which should have concerned an investor would be no defense to the charge of a violation, but would rather go to the issue of degree of enforcement response, i.e., should it be a civil or administrative action, rather than an indictment on criminal charges. In another regulatory area, a violation arises from deliberate false statements entered in the records of a bank regardless of whether or not monies are stolen.

NRC licensees must comply with a substantial body of regulatory requirements. Certainly all violations of these many requirements should not be considered to be white-collar crimes or related abuses in the

Safeguards area. However, there clearly would be an "intent to commit a wrongful act or to achieve a purpose inconsistent with law or public policy" where the offender, alone or in concert with others:

- is involved in theft or diversion of nuclear materials, or
- manipulates or alters records or reports required to be kept by his employer or by NRC, or
- makes any false report in connection with quantity, location, protective devices for movement, or authorization of movement of nuclear materials.

These criteria for wrongful intent run roughly parallel with current NRC definitions of compliance violations. NRC applies the term "violation" to situations in which there is "(i) Diversion or theft of plutonium, uranium 233, or uranium enriched by the isotope U-235 . . . . (k) Other similar items of non-compliance having actual or potential consequences of the same magnitude . . . . [or] . . . . Failure to report the above items."[15] NRC criteria for civil monetary penalties being assessed include ". . . significant items of non-compliance . . . which represent a threat to the . . . safety, or interests of the public, or to the common defense or security . . . ," and specifically where there is "a deliberate failure of a person to comply with regulatory requirements . . ."[16]

For the purpose of defining the white-collar crime problem in the area of regulating NRC licenses, the element of *intent* should be broadly construed to also cover all *deliberate* acts including omissions calculated to prevent or hinder licensees or NRC from having cognizance of facts which would lead them to take action or make further inquiries with respect to the locations, situs, or movement of nuclear materials,[17] or to the operability of protective and control equipment.

2. Disguise

The first element, *intent*, basically involves the presence of some wrongful purpose or objective. This second element, disguised purpose, involves the character of adversary implementation. When a common crime is committed, the wrongful intent is followed by an implementing act, e.g., an armed attack, which is clearly observable as such. In a white-collar crime situation the adversary does not choose to rely on force, the

---

[15]Attachment B, p. 1, A.E.C. Announcement to all A.E.C. Licensees: CRITERIA FOR DETERMINING ENFORCEMENT ACTION AND CATEGORIES OF NONCOMPLIANCE WITH A.E.C. REGULATORY REQUIREMENTS - MODIFICATIONS (Dec. 31, 1974).

[16]Ibid., p. 3.

[17]In areas of nuclear safety and quality control there could be parallel intent to commit white-collar violations.

threat of force or other overt implementing acts. *Disguise* can be defined as the facade of legitimacy imposed by the white-collar adversary on the acts employed to implement his scheme.

Disguise may take many forms. It may be written or verbal. It may rest on the authority of the adversary himself or on some claim of derivative authority. It is essential, however, that it occur in an apparently legitimate context to ensure that the victim (or victim system) responds as planned. If written materials are involved in the deception they must be delivered through customary channels or, if they are not, there must be some very plausible reason for such deviation. Only very rarely will the victim (or victim system) be called upon to respond in anything but its usual or accustomed manner.

In a bank, for example, the loan officer who creates a fictional borrower complete with promissory note, financial statement of borrower and perhaps even forged indicia of collateral, will insert these documents into regular bank loan channels. He will obtain approvals from other necessary signatories by his implicit (and unstated) assurance that the papers are authentic and that he is not acting on his own behalf. The papers will generally leave his custody (to walk them through might create suspicion or unwanted inquiries because it would be unusual). These papers, not the loan officer, will therefore move through to disbursement channels with the end result that the funds will be credited to the account of the fictional borrower from which they can easily be removed. Papers are not what they purport to be in white-collar schemes, notwithstanding the fact that they bear all the indicia of authenticity and are issued from a proper source.

Collusion by small numbers of adversaries within an organization may make it possible to execute rather complex and multi-faceted schemes. Thus in a local government social welfare program which provided jobs for disadvantaged youths, collaboration between adversaries in the personnel and computerized payroll departments made possible the issuance of payroll checks for fictional employee beneficiaries. The personnel officer generated the paper which created the employees, and the payroll computer complex processed and issued the checks. Here there was an apparently redundant system. Personnel records were based on employee records from work sites, but the two sets of records were not checked against one another. Cross-checks among redundant mechanisms must actually occur to be useful.

Collusion across organizational lines will enhance adversary ability to disguise activities on multiple fronts. For example, where a supplier (or one of its employees) enters into a scheme with the purchasing agent of its customer there are numerous opportunities for the disguises of purpose which make white-collar crimes possible. Ten units may be ordered and only five shipped, for example. With the collusion of one more person, on the

customer's receiving dock, verification for receipt of ten units which would trigger payment is accomplished. Even in the absence of such collusion, it might be possible for an insider to interpose a fraudulently prepared set of receiving verifications for the absent five units. If one supposes a reverse scenario involving a customer who wants more than he is willing to pay for and who can subvert his supplier's employee(s), a similar pattern of disguise-facilitated scheme implementation can be described.

An adversary act may be misrepresented to obtain permission to undertake some activity rather than to procure money or property. Thus a pharmaceutical manufacturer seeking regulatory consent to issue a new drug may falsify test reports or omit to state facts without which reported data would be misleading. Or an arms exporter may, as has happened, ship disassembled weapons described in shipping documents as laundry machinery, to avoid federal controls of arms exports --- deceiving shippers explicitly, and the U.S. State Department by its act of omission.

The *disguise* element in a white-collar crime scheme will often be based on some prior non-white-collar crime. For example, stolen non-negotiable stocks or bonds may not be salable but have substantial value as collateral for loans. Thus, an apparently legitimate businessman can be used as a front for making bank loans secured by the guarantee of a "friend" who will endorse stolen securities and place them with the bank as security for the loan. In one instance, bearer bonds were "borrowed" from the vault of a bank so that they could be deposited with the assets of an insurance company in the vault of another bank, allowing them to be counted among the insurance company's assets on the day when the state insurance department examiner came to take inventory. Inventories taken in two facilities, or in two parts of a facility on different days may thus create vulnerabilities --- albeit of relatively short-range duration if within a single facility between plant-wide shut-downs for inventory.

NRC-licensed enterprises operate in an atmosphere of elaborate controls and checks and balances which make it extraordinarily difficult for such disguises to succeed, but which may create a false sense of security. Protective requirements such as multiple signature authorizations and verifications, requirements that two persons be present for certain designated activities, customer-inspection presence at supplier facilities such as fuel fabricators, redundant safety and quality control inspections, procedures for frequent inventories, transaction reports to NRC and ERDA, procedures for reconciliation of relatively minute shipper-receiver differences --- all these make for very substantial differences in degree but not differences in kind from what one finds outside the nuclear industry. These differences in degree may eliminate and deter all but the most imaginative and innovative *disguise* efforts. However, one cannot be certain that in a future environment involving more massive numbers of transactions, larger numbers of potential adversaries, new motives such as those provided by expanded markets for stolen materials (all of which may challenge system functionaries to whom a disguised transaction is something they never really cope with and only rarely hear convincingly described as something which actually occurred), that such disguised transactions will not be successfully executed.

3. Reliance by Adversary on Ignorance or Carelessness of Victim

While *intent* and *disguise*, the first two elements, are clearly adversary-controlled factors, since they involve the adversary's objectives and chosen method(s) of execution, *reliance . . . . on ignorance or carelessness of the victim* (system and staff) is a victim-related element, since it is based upon victim susceptibility.[18] The susceptibility here would be a deficiency in target hardness, based on the degree of inability of the victim (system) to perceive deception, or some looseness in defensive systems for verification of paperwork or other information being handled verbally or through computers.

In many government programs protection against white-collar crime rests on post-audits or victim complaints. This is a built-in susceptibility to fraud, based upon cost-benefit or similar considerations. Thus payment will usually be made under government contracts without very close scrutiny, so long as the paperwork of the claim appears proper and there is both an absence of suspicion and some prior dealing with the claimant. Similarly, an advertiser will accept a claim and make payment on the basis of the certification of a radio or TV station that spot commercials have been broadcast in specified quantities and on specified dates, and regulatory agencies will generally authorize actions or operations of regulated entities based upon facts certified to them. This built-in susceptibility is based on the reality that agency resources will never be sufficient to investigate, or replicate by duplicate experiments, every fact reported as the basis for regulatory action. The theory on which such a regulatory approach is based is that most would-be offenders, or those through whom they must operate such as attorneys or accountants, will be deterred by the fact that post-audits or victim complaints will trigger criminal action, civil penalties, or disqualification from further access to participation in the regulated industry. In such cases, "ignorance" is not a perjorative term, since it represents a deliberate and carefully invoked policy adopted after weighing dangers of crime against (a) dollar costs to the agency of higher levels of surveillance, and (b) both dollar and intangible costs to private or commercial activity if there were minute pre-authorization inspections.

Such post-audit policies do not constitute carelessness, unless improvidently adopted or poorly executed. The adversary seeking to take advantage of this kind of policy must first calculate what he has to gain, and then hope that his illegal activity goes undiscovered on post-audit or that victims fail to learn of their victimization or have some reason not to complain.

---

[18]Another victim-related aspect, *voluntary victim action*, is discussed below.

Where policies do not rest on post-audit deterrents, but on preventive controls, individual or system carelessness will be a more important aspect of system vulnerability. Where a shipment should not leave a plant without the concurrence of specified departments or individuals, the absence of reliable procedures for ensuring that authorizing documentation is genuine and unaltered will constitute "carelessness" in this sense. "Carelessness," here, is not necessarily synonymous with negligence or culpability. Once again, cost-benefit considerations are relevant. It is not difficult to visualize a plant totally immobilized by inspectors outnumbering production personnel, watching both production personnel and each other.

The NRC cannot make cost-benefit assessments in the same manner as a government procurement office, or a financial or pharmaceutical regulatory agency. The consequences of a violation are far more serious than those in other regulatory or administrative contexts. Therefore, near-time or real-time accounting, inspection, and verification procedures will occupy a far broader portion of the spectrum of regulatory activity than will post-audit procedures.

The white-collar adversary will have to assess opportunities and dangers. Where post-audit procedures are relied on, opportunities will be perceived by the adversary to be relatively greater than the dangers. Where current, preventive controls are employed, the adversary will have to more carefully assess the possibilities of literal carelessness, gullibility, or the likelihood that redundant mechanisms operate more in theory than in fact. *Reliance*, then, is the element of offender perception of system vulnerability to subversion by guile and deceit.

4. Voluntary Victim Action to Assist the Adversary

The successful completion of a white-collar scheme is not a matter fully under the control of the white-collar adversary. The victim must *voluntarily* undertake to perform some act for the scheme to be completed. This element may have implications for those with detection and enforcement responsibilities. Measures designed to prevent inadvertent victim cooperation may be more effective than trying to predict adversary behavior.

In a common crime, the victim does not cooperate; the adversary is in control. Thus, a man with a gun at his head will comply with the demand that he part with his wallet, but it is generally both forseeable and predictable that the victim will not resist; the adversary thus controls the total situation. In executing a white-collar transaction the adversary is not in full control, but rather relies on hopes and expectations that he can prevail by virtue of what he says or does, and by virtue of the receptivity of the environment in which he operates to the methods he adopts. Even an executive at the highest levels of management, who has considerable power over his subordinates, must gain their freely given cooperation if he is to succeed as a white-collar adversary. It would be

highly dangerous for him to exercise raw power to get what he wants, since those in subordinate positions can then gain power of their own such as the power to blackmail. Or such a subordinate could take other steps, such as confidential disclosures to law enforcement agencies, regulatory agencies, or to others at high levels of management.

Thus, for a successful white-collar crime, the unlawful objective (*intent*) must be implemented by illicit methods (*disguise*) directed against some point of vulnerability determined by *reliance* where it is anticipated that the victim, or victim system will respond by taking the desired *voluntary (victim) action* to give the white-collar adversary what he wants. The *voluntary victim action* can only be based on the victim, or victim system, misperceiving the nature of what he (it) is being called upon to do.

The bank loan officer processing a loan to a fictional borrower for his own benefit will obtain another officer's approving initials because the latter erroneously believes that his fellow banker is an honest man properly handling a legitimate loan application; otherwise he would not initial the paper (unless, of course, he was in on the scheme). The regulator approving an application to release a new medication will assume that the detailed descriptive test data and results represent actual test activity, and will question test conclusions or the absence of necessary experimental steps, rather than whether the represented test actually took place or whether the observed reports were accurately reported. A securities regulatory agency will take the affirmative step of filing a registration statement, thereby permitting sale of the security to the public, if the registration statement bears all the earmarks of making a full disclosure of all the facts as reflected in the work of attorneys who prepared the statement and the accountants who certified the underlying financial data.

Since obtaining *voluntary victim action* is absolutely essential to the purpose of the white-collar adversary, any protective system must assess the possibility that it will inadvertently cooperate with and assist the white-collar adversary; the adversary's *reliance* is based on his assessments of this factor. The Safeguards system must ask questions such as: How will its representatives react to carefully prepared fraudulent documents coming to them in the regular course of business? Are authorizing documents invariably checked with their purported issuers before action is taken, or do system representatives assume that papers are what they purport to be? Does the system permit its representatives to make such assumptions? How would system representatives react if faced with a stepped-up tempo of activity during which they are asked to respond to white-collar adversary actions? Do system representatives place their major reliance on their trust in colleagues or on those with whom they customarily do business, or in prescribed protective procedures? Have there been previous situations where what appeared to be violations turned out to have been easily corrected mistakes, and what effect did these have on staff attitudes?

To the extent that a white-collar adversary group is expanded[19] to include representation across departmental lines within a facility, or among facilities or different licensed enterprises, or to include a member of a regulatory staff (as has happened in other regulatory agencies), vulnerabilities may increase by orders of magnitude.

5. Concealment of the Violation

When a violent or other common crime is committed, the offender will give very careful consideration to shielding his identity. He will act in the dark, wear a mask, perhaps even kill to prevent the survival of a witness who can point him out in a lineup. In some rare instances such offenders may have concealment of the crime itself among their objectives, such as the rare and mostly fictional instance where a murder is arranged to look like an accident or suicide. More common is the pilferer who steals small amounts which he hopes will not be missed. *Concealment* of the crime itself, from the victim as well as from law enforcement agencies, is always a white-collar adversary objective as well as an element of the crime.

The ideal white-collar crime, from the point of view of the offender, is one which will never be recognized as a crime or wrongful act. A charity fraud is ideal from this point of view: small amounts are taken from large numbers, and no victim has a sufficient interest to pursue the matter even if he suspects he has been defrauded. In anti-trust or price-fixing cases, every effort is made by co-conspirators to make the public, regulators and law enforcement agencies, believe that normal market forces determine the prices they pay, rather than illegal agreements. Some investment frauds are predicated on the perpetrators' assumption that they can use the scheme proceeds to "make a killing" on some speculative investment, square accounts with their victims, and thus prevent the day of reckoning.

Concealment plans can sometimes be supplemented by post-disclosure contingency plans. In some instances where victims invest money in business opportunities, victims will frequently be mobilized by the man who cheated them to come to his defense after his indictment, trading on their refusal to see a dream die and to face the fact that they have been swindled. In other instances victims fear the consequences of their victimization; disclosure might mean that they will be suspected of being negligent managers and will lose their jobs or be subjected to legal action --- such victims sometimes can be depended upon to cover up the fact that a crime has been committed.

---

[19]It should be recognized that while vulnerabilities of protected facilities will be greatly increased if such a situation were to develop, the white-collar adversary is also exposed to greater risk in such a situation. See p. III-4, supra.

Concealment is especially important to the white-collar adversary because he operates in the open. He cannot obtain victim cooperation by wearing a mask. His objectives are only sometimes short-run; embezzlers often work at their thefts over periods of years, and sometimes decades. In one major fraud case counsel for the defendant argued that his client had a clean record, was a regular church-goer and pillar of the community. The judge responded: "Who else could have committed this kind of crime? A street criminal?" The adversary will often be a respectable member of the community with strong personal, professional, and business ties. *Concealment* is essential to his ability to maintain his position in the community, his ability to repeat his crimes, or both.

The white-collar adversary may recognize that he cannot always permanently cover up his crime, and so *concealment* may become an objective of flexible dimensions. If the crime cannot be concealed forever, can it be concealed long enough to amass sufficient funds to finance a short or long-term foreign haven?[20] Sometimes the scheme itself is based on the expectation that a sufficiently expanding group of victims can be lured into the net, so that the money obtained from later victims will be used in part to keep earlier victims from knowing they have been cheated.[21] These schemes must eventually fail because of the mathematical progression involved, but some such schemes have continued for many years.

The varied dimensions of concealment can be seen in white-collar crimes with very limited objectives. Many check-kiters, for example, have as their objective no more than a loan to which their credit rating does not entitle them. Needing operating capital to finance their businesses during production and before payments will be received they may open multiple bank accounts, write checks from one to the other in large amounts, depending on the fact that each bank credits them with funds while waiting for the deposited checks to clear. If the hoped-for payments arrive, accounts are settled and the check-kiter has deceived his bank into giving him an interest-free loan in a situation where it would not have given him a conventional loan. If the busy check movement schedule is interrupted for any reason, the entire operation collapses and the check-kiter is exposed.

The check-kiter is one type of white-collar adversary whose objective is to buy time while trying to solve a business or personal problem. Other types include the businessman whose enterprise is failing, and who buys on credit and sells below cost, for example, using his credit purchases to raise operating capital, and frequently ends up as a fraudulent bankrupt.

---

[20]Some fugitive financiers were able to prolong their Brazilian havens for many years after discovery. Fugitive Robert Vesco has established a sufficiently strong economic base in Costa Rica to withstand the most strenuous efforts of the U.S. Government to extradite him or recapture stolen funds.

[21]This is called a Ponzi Scheme, named after one of its most famous practitioners.

In all these instances *concealment* is a key objective. *Concealment* only rarely involves hiding one's true identity. Rather, it is confined to measures taken to hide the fact that a crime has been committed. It differs from *disguise*, the second element discussed above. The purpose of *disguise* is to consummate the crime; it is part of the manner and means by which the fraud is committed. To the extent that the fraud is a continuing one, *concealment* and *disguise* will overlap, since putting off pursuit and maintenance of the facade of respectability is the manner and means by which iterations of the fraud may be inflicted on old and new victims. Even where there is no intent to commit further white-collar crimes, however, *concealment* will be a continuing element of the crime. It may result in new crimes to cover up old crimes, i.e., continuous repetitive alteration and falsification of records or, as discussed above, new thefts to pay off old victims.

The *concealment* element is one which merits emphasis in this report because it has particular relevance in the area of regulation of nuclear enterprises. If there is a diversion of nuclear materials from the possession of a licensee, committed by guile and deception rather than force, the white-collar adversary group is most likely to include employees or managers or licensees and/or suppliers of goods or services to such licensees. These are likely to be individuals with families and roots in the community for whom *concealment* will be a major objective. It is also likely, as will be discussed below,[22] that their motivations will often be quite complex, and intentions ambivalent.

These five elements of white-collar crime have been addressed in some depth because they help to define the problem of white-collar crime in the nuclear area, and thereby give some direction to the planning and design of countermeasures to cope with the white-collar adversary.

The general elements of white-collar crime are, as has been noted at several points in this chapter, relevant to Safeguard issues, and there is no reason to develop a list of elements of this form of crime specially tailored to the problem of nuclear Safeguards. However, it should be recognized that the spectrum of white-collar crime is very broad, and that the elements noted above have different significance when applied to different forms of white-collar crime. This can be illustrated by reference to particular classifications of white-collar crime.[23]

In the case of individual, ad hoc crimes such as personal income tax violations, *disguise* will consist principally of omissions, *reliance* is based on automatic *voluntary victim action*, and *concealment* rests not on

---

[22]See Section IV, pp. 12-30.

[23]Edelhertz, op. cit., at pp. 19-20.

some adversary action but on his assessment of the statistical odds that the return will not be audited, and that the auditing process will not clearly establish the violation even if an audit takes place. In abuses of trust situations, where the white-collar adversary is an employee or fiduciary who has taken advantage of employer or client there is likely to be a rather elaborate facade involving *disguise* and *concealment*. Where the white-collar adversary has committed a crime incidental to and in furtherance of business operations, but where crime is not the central purpose of his business operation (e.g., an anti-trust violation), *disguise* and *concealment* will be undertaken in a subtle and sophisticated fashion, all the more so because the adversary does not conceive of himself as a criminal and his wrongful acts will be inextricably intertwined with entirely legitimate business operations. In con games, where the white-collar adversary has no business other than to use guile and deception to take the money or property of others, *disguise* will be more blatant, *concealment* more contrived, and the adversary will be likely to be highly mobile, moving from place to place to find new victims.

If white-collar crimes or related violations are currently being committed in the areas of concern to NRC Safeguards program, or if such crimes and related violations are committed in the future, these elements (though all present) will be present and operate in ways which reflect unique vulnerabilities of the nuclear regulatory system to fraud and deception.

It is highly unlikely that white-collar adversaries can operate without some base in (or performing some service for) the nuclear industry or NRC itself. Any white-collar adversary group is therefore likely to contain one or more individuals who have established positions in or close to the nuclear industry. This has several implications.

First, *concealment* will be an overriding objective. If the theft, diversion, or cover-up of unaccounted-for nuclear materials is continued and repeated, *concealment* will both protect the position of the insider and make it possible for him to continue.

Second, the expected white-collar adversary may have a broad range of motivations for formation of his *intent*. His motive may be to protect his job, or his employer, as well as to steal or divert nuclear materials.[24]

Third, the white-collar adversary is more subject to deterrence and frustration than the adversary who will use force, since he must procure *voluntary victim action* (from some individual or system) to be successful.

---

[24]Section IV, at pp. 12-30.

Effective education and orientation increasing the sensitivity of nuclear industry personnel to the white-collar adversary would make it more difficult for this adversary to obtain needed voluntary victim action. The white-collar adversary must also be able to rely on either *concealment* of the crime or violation, or a combination of delay and obfuscation of the trail which will prevent his identification.

Fourth, if the white-collar adversary succeeds in stealing or diverting nuclear materials, these materials are probably less likely to end up in the possession of terrorists or extortionists, than are materials stolen by other means. The *concealment* element would be seriously undercut by such an end-use; the same would be true of black marketing which could result in such an end-use.[25]

* * *

Safeguards system design should take into account the above elements of white-collar crime, and the nature and character of potential white-collar adversaries discussed below.

---

[25]This does not preclude the possibility that given sufficient financial incentive and assurances of concealment, or coercion through blackmail or otherwise, that nuclear materials would not be supplied to terrorists or extortionists by the white-collar adversary. See Note 11, supra.

IV. CONCEPTUAL SCHEMA OF WHITE-COLLAR THREATS TO THE NUCLEAR INDUSTRY

As noted earlier, unlike other potential threats to the safeguarding of nuclear facilities and material, the white-collar challenge has been little probed and explored. This has been due largely to two factors. First, threat analyses have focused the greatest amount of attention on more observable and more easily conceptualized adversaries such as the terrorist or other armed assailant. Second, the developmental history of the nuclear industry has been one in which a high degree of interpersonal trust between the private and public sectors fostered --- in a climate of secrecy and high security --- the evolution of a destructive force into a constructive power technology. This developmental bond of trust, combined with the high intrinsic value of materials licensed to private sector individual firms, have tended to focus consideration of Safeguards threats on "outsider" adversaries --- not privy to or respectful of the long history of a secure and integrity-bound public-private partnership.

Against this backdrop, the issue of a white-collar threat is both anomalous and bothersome. The white-collar adversary, by definition, is not likely to launch a direct assault against a nuclear facility or one that is easily observed or detected. His tools will not be those of force or violence but those of deception, manipulation, and falsification. He will work not from the outside but from inside the industry or its regulatory structure. He will be one of the trusted rather than one of the suspected or feared.

To conceive of the white-collar adversary in this way is not to say that he or she now exists or ever will exist. A failure to face the white-collar challenge at all, however, is to ignore a potential Safeguards threat. The consequences of a deceitful manipulation of nuclear material by facility insiders can have consequences as disastrous as a direct armed assault on a facility by outsiders --- regardless of how equally remote these two events are or seem to be.

Considering the white-collar threat, then, is not to concede its existence any more than a consideration of a 12-person armed assault on a facility is to suggest that this has occurred or is likely to occur. Rather a probe of the white-collar adversary is but another test of the Safeguards system --- its detection potential and its resiliency. It helps develop a general assessment of the preparedness of Safeguards systems and procedures to cope with the full range of threats and with all potential adversaries. It should also help to avoid the danger that some adversaries will get disproportionate attention because the system is more likely to know how to cope with them. What follows is a conceptual schema by which nuclear Safeguards systems and procedures can be

probed from a white-collar threat perspective. It is intended to be a conceptual guide to assist assessment of Safeguards preparedness to counter this threat.

This schema is divided into three parts. Part 1, "The White-Collar Adversary," describes those characteristics of the adversary that both are and are not relevant to a white-collar Safeguards assessment. Part 2, "Motivational/Opportunity Structures and Related Adversary Objectives," presents the likely motivational structures to which potential adversaries may be expected to relate. Part 3, "Implementing Acts and Actions," is a description of the quality and nature of representative white-collar acts that might be undertaken to achieve wrongful adversary objectives.

A. THE WHITE-COLLAR ADVERSARY

As noted earlier, the white-collar adversary to the safeguarding of nuclear facilities and material is far less likely to be an outsider, i.e., an individual or group subversive or terrorist in nature or unrelated to the nuclear industry, than is the case with other potential sources of threat. The most credible white-collar threats will arise from two sources: (1) those within the nuclear industry or regulatory structure itself; and (2) those outside the industry working through insiders. The possibility of system manipulation, deception, and/or falsification characteristic of the white-collar adversary is credible only if the adversary has an intimate knowledge of and requisite experience with the system(s) and procedures to be manipulated.

For our purposes here, the term "adversary" is used as a collective noun representing an indeterminate number of participants. There are three reasons for this. First, full-blown scenario development complete with defined parameters on size of an adversary force are premature at this time and in any case clearly beyond the purview of this initial study of the nuclear white-collar challenge. Second, and equally important, is the fact that unlike armed adversaries launching a direct assault on the nuclear industry, the white-collar adversary's success does not so directly depend upon the size of an attack team. More important than the number of participants involved in a white-collar threat are the nature, authority structure, and operational bases of those participating. Strategic location of the adversary in a facility or in the industry itself is more significant than the number of co-conspirators. Similarly, the sources of individual authority possessed by the adversary can often obviate the need for additional partners. In addition, unlike the outside adversary attempting an armed assault on a nuclear facility or vehicle and for which the addition of extra manpower can mean the difference between success and failure, an internally generated white-collar "assault" on the nuclear industry may be positively jeopardized by the addition of conspirators. The more people involved in a fraudulent action, the more risky it becomes and the more difficult it is to control their varied actions and behaviors.

Many a white-collar scheme that could have continued indefinitely has been blown wide open because one minor individual became nervous. Often these individuals were not keys to the scheme, but were made privy to it to avoid additional cover-up activities that the major conspirators found too time-consuming to attend to. The number of participants, then, is not necessarily a relevant parameter for use in investigating the white-collar threat.

Finally, characterization of varying threat potentials of the white-collar adversary in terms of the number of participants involved can be made additionally irrelevant by the fact that a competent adversary may be able to exert the force of many through the fraudulent misrepresentation of bonafide authority or the authority of others. For example, someone with the power to authorize an external shipment of nuclear material (or the ability to successfully misrepresent that authority) would not necessarily need the collusive participation of others in the facility who would actually prepare, handle and carry out that order. As long as the authorization was correct and in order, they would proceed in good faith to carry out all procedures as directed.[26] On discovery, the scheme might appear to have many handmaidens when in fact a single or small number of participants was able to act with the force of many. The size of the white-collar adversary, then, is unlikely to be as critical to its threat potential as the significance of its strategic location, sources of power and/or capacity to fraudulently misrepresent authority.

The following adversary characteristics are significant in assessing the potentials of a white-collar threat:

- Capacity to access "attractive" nuclear material or important records thereof;
- Susceptibility to detection; and
- Probability of detection.

Each of these characteristics is discussed in turn below.

1. Capacity to Access "Attractive" Nuclear Material or Important Records Thereof. From a white-collar perspective, the adversary characteristic of capacity to access involves three dimensions. The first of these is the most obvious --- actual physical access to and control over material or records. Considering organizations as a whole rather than just plant production personnel, it is likely that individuals having direct access to

---

[26]Here we refer to how nuclear materials can be removed from a facility; it is recognized that any scheme would have to also consider how to block subsequent awareness that it is missing or did not arrive at its purported destination.

records are greater in number than those having physical access to materials with some overlap among individuals with custodial functions.

The second dimension of the adversary's accessing capacity is the power to authorize movements of material within a licensed facility, i.e., internal movements. Authorizing power gives the potential adversary access to material not in the physical sense but in the sense of allowing him/her/them to exert effective control over that material and its movement pattern(s).

The third dimension of this adversary characteristic consists of the power to authorize movements of material into and out of a licensed facility, i.e., external movements. Again, such power does not involve physical access but the capacity to exert effective control over material/product movement(s).

Capacity to access may be greater where it is most indirect. In an attempted diversion of material, for example, an individual with direct physical access would be likely to successfully remove only small amounts of the material under his direct physical control. An individual with authorizing power, on the other hand, could "access" larger intact quantities of material by directing the time and place of their movements. An order "through channels" might well trigger less suspicion than one personally given. The more indirect the capacity to access, then, the greater the potential range of control an adversary might be able to exert for wrongful purposes.

An important consideration in determining the access capacity potential of the white-collar adversary is thoughtful anticipation of those targets (nuclear materials or information) which he might define as "attractive." To large extent, the attractiveness of various targets will be determined by the adversary's motives and objectives --- subjects to be covered in the following sections. Grading of Safeguards attractiveness has been extensively studied in connection with systems design and the formulation of Safeguards objectives and policies. It should be noted, however, that the range of targets attractive to the white-collar adversary is not necessarily the same as that of other adversaries. To begin with, for example, the terrorist adversary is likely to have only one primary object that is attractive to him --- a significant amount of Pu or other dangerous material. The white-collar adversary may find certain records as "attractive" as material of any kind for his purposes. Thus, the range of potential adversary targets is much broader for the white-collar threatening source than for other adversaries.

Similarly, the white-collar adversary's definition of what material is attractive may differ significantly from that of other adversaries or from that of NRC for that matter. At the present time, the graded Safeguards system employed by NRC through its regulatory structure is in a very real

sense NRC's definition of material attractiveness. The level and kind of material accounting and controls which the agency applies to the various grades and kinds of nuclear materials is only its assessment of the relative values and Safeguards risks of various materials. To a large extent, these definitions derive from conceptions of particular adversaries and their perceived end uses for various material. Thus, the safeguarding of Pu carries the strictest and closest accountancy requirements, since the prevention of terrorist groups from gaining access to armament material has been and will continue to be a major Safeguards priority.

For the white-collar adversary, however, the present graded Safeguards regulations may not represent an ordered hierarchy of material attractiveness. For him, material that can serve to solve an administrative or management problem may be far more attractive than that which can be used to make a bomb. Or alternatively, bomb-grade material may only become attractive because it can assist in solving a particular problem, e.g., nuclear material accounting discrepancies. In addition, the white-collar adversary is likely for the short run to be far more interested in the location, movement and proportional relationships in amounts and kinds of material present in a facility than in its relative value or worth. Attractiveness of various types of material then, may be derived more from their manipulative potential than from an invariable perception of their end use.

Finally, the relative attractiveness of given materials and products in the nuclear fuel cycle is likely to undergo considerably more flux where the white-collar adversary is concerned than is true with other threat sources. This is because as rapid industry growth occurs, the white-collar adversary will quickly react to the new and developing commercial value of accessible objects. The terrorist or other adversary possessed of a narrow range of objectives will have far greater stability in his threat targets. This is why anticipation of material attractiveness is so critical to understanding the access potential of the white-collar adversary. It means continual re-evaluation and re-interpretation of Safeguards systems and regulations, particularly with regard to their implied material attractiveness definitions. It means that the regulator concerned with Safeguards must keep fully apprised of and informed about the economics of the nuclear industry, as well as its technology. Finally, it means that the design of Safeguards systems and procedures must anticipate new relationships among emphases and uses of various materials, products and records.

2. Susceptibility of The White-Collar Adversary to Detection for Adversary Acts/Actions. A second adversary characteristic bearing on the potential of a white-collar threat concerns the susceptibility to detection of relevant actors in the nuclear industry. Unlike capacity to access attractive material or records which is a job-related adversary attribute, susceptibility to detection is an adversary characteristic determined by the Safeguards system itself. It is, in effect, an assessment of the Safeguards system which the adversary must himself make since it bears on

his capability to successfully carry out adversary acts of a white-collar nature.[27]

(a) Actual versus perceived susceptibility to detection. An adversary's actual detection susceptibility may not be as important as the perception he has of that susceptibility. This is in some ways very fortunate since it is likely to be impossible -- if not cost-prohibitive --- to design a material accounting and records control system which applies an equal and high degree of detection sensitivity to all participants and transactions. It should be recognized, however, that the white-collar adversary will be extremely sensitive to whatever degree of detectability does exist. This is true for several reasons.

First, the white-collar adversary --- unlike the armed or terrorist adversary --- intends an act that is covert in nature, i.e., that will not be detected. This places detection and its avoidance uppermost in his mind. Second, this adversary may not conceive of himself as an adversary, making him extremely sensitive to being detected in the performance of "adversary-like" actions which would cost severely in self-esteem and/or loss of employment. Finally, the ultimate success of the white-collar adversary will frequently depend upon maintenance of his professional position in the system which he has learned to manipulate. Detection would result in certain expulsion from that position and ultimate failure in achieving his adversary ends.

(b) Sensitivity to detection and credible detection capacity. Because the white-collar adversary is sensitive to detection susceptibility does not mean that he is easily deterred on that basis. On the contrary, what it does mean is that he will assess carefully his susceptibilities and the sources from which they derive. If he is inside the system he will have both opportunity and time to make an in-depth study of this crucial issue. Because the white-collar adversary, then, will be something of an expert on his susceptibility to detection, attempts to create illusory system capacity to detect are extremely self-defeating. Institutions and organizations in which a high degree of individual integrity is necessary often try to enforce compliance with rules and regulations by frightening their employees with a managerial capacity to check up on them which, while apparently significant, is in fact illusory. A deterrent, like a threat, is only effective when credible. The attempt to make credible what is an imaginary capacity to detect is ultimately self-defeating. The white-collar adversary, for example, rather than taking the system at its word, is far more likely to test it as discussed below and discover the disparity between the bluff and reality. Once having done so, he has gained an upper hand on the system attempting to control his actions.

---

[27]It has been noted that the higher the adversary's perceived level of susceptibility to detection, the less his adversary potential. See USERDA Report ERDA-7, op. cit., Note 6, at p. I-3, pp. 17-20.

Rather than trying to achieve a degree of system sensitivity that makes all participants equally and highly detectable or attempting to "impress" employees with non-credible detection powers, Safeguards authorities are better advised to approach the detection sensitivity of the white-collar adversary by pursuit of efforts in two areas: (i) multiplication of the number and level of those points at which detection can occur; and (ii) consistent, timely, and imaginative use of detection mechanisms already available.

Increasing the number of points at which the system is made detection-sensitive positively affects the susceptibility of an adversary. This is because the scope of the adversary act is concommitantly increased. Increasing the number of levels at which detection may occur precludes the situation in which all possible detections are made within a subsystem over which the adversary has or can exert ultimate control. At the same time, the design of a detection system cannot be divorced from its utilization. No matter how sophisticated and sensitive the detection mechanisms of a nuclear Safeguards system, if they are not invoked consistently and in a timely fashion, or invoked only lackadaisically, they will not be effective. Failure to respond to the discovery of an error, a discrepancy or an irregularity --- no matter how minor --- is both a failure in detection and a possible incentive to an insider to become an adversary. Inconsistent or time-lagged responsiveness at minimum suggests system weakness or lack of resolve; and at worst, provides the adversary with information relating to the tolerance levels of detection system sensitivity.

Utilization of detection potential is especially critical where the white-collar adversary is concerned. This is because this adversary is quite likely to probe the system for its sensitivity and to get a current reading on his detection susceptibility. If he sends through a record with a minor clerical error, for example, it is unlikely to have substantial negative consequences if detected. The way in which it is detected and investigated (if at all) can give the adversary valuable information about detection mechanisms and the resolve with which they will be invoked. Such a testing of the waters also provides the adversary with considerable information about the degree to which he is susceptible to detection and the time frame in which detection is likely to occur.

The more consistent and more timely the invocation of a detection system response, the more sensitive that system ultimately is, the less it will tolerate, and the more susceptible those attempting to subvert it become to detection. For the white-collar adversary such a system is troublesome. Without fail, this adversary will make an informed assessment of the systems which confront him; Safeguards authorities should not fail to do the same.

(c) Two general propositions on susceptibility to detection. Having described the importance of detection-avoidance to the white-collar adversary and the elements of detection mechanisms to which he may be most responsive, it is appropriate now to further characterize white-collar adversary potential within the dimension of susceptibility to detection. Important susceptibility attributes can be described by the statement of two general

propositions:

> Proposition 1: Given similar and adequate access attributes, the white-collar adversary with authority to correct, verify, edit and/or reconcile discrepancy or error will be relatively less susceptible to detection than are those whose work he monitors.

The essence of this proposition is that those who perform originating functions or generate original records will possess a greater susceptibility to detection for the introduction of discrepancy or error than those performing verification or feedback functions or generating secondary though independent records, for example those maintaining computerized records. The authority to error correct and/or reconcile differences provides as well a relatively less detectable capacity to introduce new error or discrepancy. Those who participate both in originating functions and in reconciling activities, present the greatest challenge to detection mechanisms from a susceptibility standpoint.

The issue raised by this proposition is the degree to which "independent measurement or verification" is truly independent in the sense of being neutral, or whether it may be characterized by an independence which constitutes a separate agenda of its own. Where, then, there exists an independent motivation to bias or misrepresent quantities of material on hand, e.g., within the error correction function, the authority to perform that task may provide the opportunity to introduce errors of omission or commission.

> Proposition 2: Given similar and adequate access attributes, the white-collar adversary performing a function(s) in which the expectation of error or discrepancy is great will be relatively less susceptible to detection than one performing in an area where error expectation is small.

The technology of the nuclear industry represents a significant challenge to material control and accounting authorities. Many of the essential elements of the technology and its basic productive processes make it impossible to precisely inventory material on hand, in process, in waste-storage or elsewhere. Sufficiently precise measurements by non-destructive means have --- and undoubtedly will continue to --- eluded technicians. Because of the impossibility of precise measurements, efforts of Safeguards authorities have focused upon the development of sampling and assay techniques and the establishment of error tolerance levels for the purpose of maintaining appropriate material control and accounting. Nevertheless, the measurement limitations of current technology are such that the expectation of some discrepancy and/or error in successive measures or counts within a process period is both real and reasonable, and represents a weakness that can be exploited. The point addressed in Proposition 2 is not

only that potential exploitation is likely to be least detectable at those junctures where the expectation of error is greatest, but that those who perform functions of which error or discrepancy is an expected part and who know well the limits of that expectation, will be less detectable and more capable of maintaining the manipulation within "tolerable" limits.

3. Probability of Detection of the White-Collar Adversary for Acts/Actions. Closely related to an adversary's susceptibility to detection is the likelihood or probability that he will be detected in the course of or after performance of an adversary act or sequence of acts. Probability of detection is largely an attribute conferred on the adversary by the system or systems in which he operates (here the Safeguards system). The likelihood of detection is an assessment that both the adversary and Safeguards authorities must make qualitatively if not quantitatively, if each is to succeed in achieving their goals.

Techniques for assessing the probability of detection for a wide variety of threats and operational situations have been extensively studied. In general, the result for the white-collar threat will be related to many factors, among which are: the number of checks or verifications to which an adversary's work is subjected; the frequency of those checks (both over time and in relation to each other); the content and sufficiency of the checks; the traceability of problems discovered in a check; the presence of extraneous events affecting the check process; and the immutable quality of checking procedures. Each will be discussed in turn.

(a) The number of checks on an adversary's work. Practically speaking, an adversary's probability of detection increases as the number of checks on his activities increases. This is true only, however, if: 1) some or all of the checks are totally independent of reliance on his work; and 2) some or all of the checks occur within functional areas or subsystems over which he neither has nor can exert control. The situation is similar to that which has been pointed out frequently in terms of the level of independent verification contributed by a state system to an international inspection where the state may be considered an adversary. Checks or verifications which rely totally or partially on the acts of an adversary may not contribute to an enhancement of his likelihood of detection since he may be able to control the "base line" on which they are made. Similarly, checks or verifications occurring in areas or by individuals under the adversary's authority and control cannot be relied on to increase his detection probability. It is important that the capability to make numbers of checks is not confused with the likelihood that they will be made. In one instance NRC was advised that computer fraud was unlikely to be a significant threat because all inputs to computers are based on underlying documentation, a comparison of which with computer data would disclose manipulations. If this were an accurate view, many of the computer frauds already disclosed in non-nuclear fields could not have taken place. In fact, the cost-benefit ratio of constant checking between input data and underlying originating data has been such, in industries outside the nuclear field that continuous checking did not proceed in a timely enough fashion to prevent frauds from taking place.

(b) The frequency of checks made. The frequency of checks over time, given that they are sufficiently independent of a potential adversary, may serve to increase the likelihood of detection. The reason frequency of checks is believed to be probabilistic is that frequency alone will not enhance detection. Rather, detectability will increase where and if the frequency of checks obliges the adversary to enlarge the scope or number of adversary acts, thereby increasing the possibility of error on his part. It is the necessary adversary response to frequency of checking procedures, rather than the frequency of the procedures themselves, therefore, which increases detection probability.

Often the frequency of checks over time is not as important from a white-collar threat perspective as their frequency in relationship to each other. Thus, for example, where an adversary's work is subject to one set of checks relating to bi-monthly physical inventories and to another set of verifications relating to weekly material balance procedures, the frequency of each set of checks may not be as significant as the extent to which they do or do not coincide in time. In other words, increasing the frequency of one or both sets of checks (i.e., making physical inventories monthly and material balances daily) may be less likely to enhance detection of the white-collar adversary than changes in the schedules of each set of checks. Scheduling weekly checks so as not to correspond with monthly inventories, for example, may greatly complicate the adversary's capacity to avoid detection. On the other hand, the existence of coincidental checks may make the adversary's task easier by scheduling his manipulative acts into predefined blocks of time.[28]

(c) The content and sufficiency of checks. No matter how many or how frequent (in either sense) checks on a potential adversary are, unless they are of sufficient content and substance they will contribute little to detecting the white-collar adversary. This adversary is greatly aided by verification procedures that are routinized and essentially perfunctory in nature, which is one reason why he presents such a significant challenge. Most control and production systems outside the nuclear industry try to achieve routinization in order to increase work efficiency and productivity. In addition, familiarity with procedures when combined with increased volume of activity seems to breed routinization and perfunctory performance of many tasks in most institutional settings. Safeguards authorities should be alert and sensitive to this problem, particularly in view of anticipated future expansion.

---

[28]It should be recognized that improved steps toward real-time accounting are likely to benefit material control and accountancy functions, but cannot be relied on to detect or deter the white-collar adversary to the same degree as the petty pilferer. The manner in which this adversary operates makes him as fully capable of manipulating a real-time system as any other.

Such checking and verification procedures as do exist should be bona-fide in nature to begin with and not allowed to become devoid of content because of routinized or perfunctory performance. "Content" in this case refers to the consistent attention to the authenticity of source and supporting documents accompanying a record. When a "check" looks only for what it expects to find on a record and eschews further available probing it has become devoid of content. Verification or checking procedures cannot be allowed to evolve to the point of becoming quick perusals of self-fulfilling prophecies. The white-collar adversary can too easily conform to such prophecies and remain undetected, for the world of exploiting the difference between reality and its representation on paper is his realm. Those with responsibility for checking procedures must constantly ask the question: Does this record truly represent what it purports to represent? And then they must probe to be sure it does.

(d) Traceability of check procedures. Another factor influencing the white-collar adversary's detection probability is the extent to which checks which do occur allow discovered problems to be traced to their probable sources. Effective checking procedures from the white-collar threat perspective are those which allow a discovered error or discrepancy to be laid at the doorstep of he (or those) who is (are) responsible for it, or in whose name it was accomplished.

The capacity to retrace events and assign responsibility for acts in a sequence, significantly increases the likelihood of an adversary's detection, once a problem has been uncovered. Often systems are effective in retracing steps in the short run (within real-time, for example) but become relatively less effective with the passage of time. Traceability which becomes less potent over time represents a vulnerability to the white-collar adversary. It tells him that his detection probability is transitory and sharply diminishing in nature. Once he passes a given period of time, he need not worry about detection since problems cannot be attributed to him. The most serious situation from a Safeguards standpoint would be one where that period of time within which traceability is possible is less than the elapsed time between normal checkpoints.

(e) The presence of extraneous events. Extraneous events that divert Safeguards authorities from their normal patterns of surveillance can significantly diminish their potential to deter the white-collar adversary. Such events may be quite unrelated to the adversary's area of activity or function. A minor fire, for example, or a health and safety criticality alert, may sufficiently divert attention generally in a facility. The white-collar adversary may stage such events himself or merely take advantage of them, but to the extent that they result in reduced attention to detail, they may give him an opportunity to operate. In addition, his act(s) may remain undetected since discovered problems may be attributed to the general confusion of the time period rather than to purposeful, adversary action. But even where some purposeful adversary action may be uncovered, extraneous events may frustrate identification of the adversary.

(f) The rigor of adherence to procedure. Finally, the immutable quality of verification, checking and Safeguards procedures and processes will affect the white-collar adversary's probability of detection. "Immutability" in this case refers to the degree to which adherence to such procedures is stringently, consistently, and without fail required of *everyone, every time* and in *every place*. Anything less than this standard will serve to diminish a white-collar adversary's detection probability. Where, for example, authority can overcome procedure, this standard will not be met. Thus, the same strictures applied to an MBA custodian must apply equally and immutably to a corporate vice-president. Situations in which lower level employees "cut corners" in the name of higher authority are extremely vulnerable to the white-collar adversary. High level managers who attempt to invoke authority in this manner (no matter how legitimate the purpose) are themselves a Safeguards threat in the sense of the climate they create. "Special conditions" (i.e., the existence of extraordinary circumstances that are believed to call for special responses) are another example of the kind of situation that should not be allowed to disturb the immutable quality of Safeguards regulations and procedures.

B. WHITE-COLLAR MOTIVATIONAL/OPPORTUNITY STRUCTURES AND RELATED ADVERSARY OBJECTIVES

It is both operationally and conceptually quite difficult to divorce adversary characteristics which bear essentially on opportunity and threat capability from the motivations that may induce an adversary to use his potential. In common crime, the essence of an offense is summed up as motive plus opportunity, a principle that applies to all criminal behavior, as well as to inappropriate or improper conduct. In the nuclear industry, there may be those who possess the capability and the opportunity to circumvent Safeguards systems and protocols in some fashion but who have absolutely no motivation to do so. Alternatively, there may be those within the nuclear industry with substantial motivation to manipulate nuclear material transactions but who have not a glimmer of a credible capacity or opportunity to act on those motives. Dangers arise obviously where those with the relevant capacity and opportunity acquire sufficient motivation. Or, as may be the case, where those inside the system confront a situation in which they are motivated to some improper or illegal conduct, and "discover" that they have the capacity to carry it out.

It should be noted that unlike the terrorist adversary who sees himself as a subversive and opposing force from the very beginning, the individual white-collar adversary may never have initially viewed himself as or intended to become such. Rather, he may in the course of his totally proper activities have discovered a weakness in the system. Then, possibly much later and under entirely different circumstances, he may be sufficiently motivated to exploit that earlier-discovered weakness. Even then he may be proceeding on motives which he recognizes as improper, but which he feels are not truly

criminal, and which may be rationalized in some manner. From here, it is not a large step to further or consistently invoke the exploitative action sequence at any hint of difficulty or for purely illicit ends. The white-collar adversary, then, while not likely to have begun with a desire or intention to weaken or subvert his position and his industry, may become a most potent threat to its well-being. This is why, no matter how remote the intersections of requisite opportunity and motive for white-collar adversary actions may seem, they must be squarely faced. The consequences of successful acts on the part of such an adversary take on a compelling urgency in an industry likely to experience a growth rate of geometric proportions over the next two decades.

Most of the motivational structures in which the white-collar adversary operates, then, may not in and of themselves be wrongful or improper. They may, in fact, be entirely consistent with the expectations of employers or regulators for proper employee conduct. It is when such proper motives become objectified in conduct contrary to internal and external Safeguards requirements that an adversary sequence arises. Thus, a single apprcpriate motivational pattern can generate a range of both proper and improper objectives or ends. An improper motive, on the other hand, can only give rise to a set of inappropriate ends.

Described below is a set of motivational structures to which some individuals within the nuclear industry might possibly respond both now and in the future. These motivational structures are divided into three groups: (1) those motives that are system-generated (i.e., engendered by internal and external regulatory pressures); (2) those motives that are position-generated (i.e., engendered by individualized responses to internal and external licensee pressures); and (3) those motives that are individually-generated (i.e., engendered by purely personal needs and desires). Practically speaking, system-generated and position-generated motivational structures are quite similar and are responsive to essentially the same perceived pressures for accountability and accuracy. The difference is that system-generated motivations represent more generalized concerns, while position-generated motivations represent similar concerns interpreted on a personal level. It is the difference between concern for one's firm or industry and concern for one's job, section or position within that firm or industry. Thus, those motivated by a generalized concern for continued smooth operations, without regulatory difficulties or interference are responding to system-generated pressures. Those motivated by a concern that any interruption in smooth operation resulting in regulatory interference not be attributed to them or their section of a facility are responding to a position-oriented interpretation of these same pressures.

Each of the motivational structures attributed to the white-collar adversary receives separate treatment below. Following each discussion, specific motives identified within each structure, together with their related adversary objectives, are summarized in tabular form. It should

be clearly understood that these descriptions are listing of *possibilities;* there is no basis at this time for an assessment as to the *likelihood* of adversaries acting on these motives.

1. System-Generated Motivational Structures of the White-Collar Adversary. As suggested above, the system-generated motives of the white-collar adversary derive from generalized interpretations of both internal and external pressures for accuracy and accountability. The adversary acting in terms of system-generated motivations is least likely to conceive of himself as an adversary. His overwhelming concerns will be for his firm and his industry, for which he will have a protective instinct. He believes strongly in the safety and security of his industry and his part of it, and even where he may feel that many Safeguards regulations are unnecessary or overreaching, he will endeavor to comply with them to the best of his ability.

For the most part he will have little difficulty in doing so. Safeguards regulations, either internally or externally generated, may be bothersome, but compliance with them is a manageable task --- so long, that is, as operations go smoothly and no unanticipated events occur. It is when things go awry --- a larger than expected MUF appears, for example, or a scheduled physical inventory reveals a discrepancy between actual and recorded materials on hand --- that his diligence, concern, and protective instincts can move him to an adversarial posture.

Four prime system-generated motivations, capable of being objectified into adversary acts, might influence the potential white-collar adversary: (a) the need to "buy time" to figure out the reason for errors or discrepancies; (b) the desire to protect the operating license of the facility; (c) the desire to protect the larger organization or the nuclear component of the larger organization from adverse pressures; and (d) the desire to advance the long term goals of the organization or component thereof. Each of these is discussed in turn below.

(a) The motivation to "buy time." The motivation to "buy time" can be distinguished from the other three system-generated motivations of the potential white-collar adversary by its time frame. Generally, buying time is a motivation with short term objectives while the others have longer range goals. Thus, the white-collar adversary with a motive to buy time wants to do so in reference to some event scheduled, or likely to occur, in the near future --- an event that he would prefer to postpone, but for which he will now need to "specially" prepare. For example, a finance manager in the course of a routine audit may discover a significant disparity between measured and book assets. He has seen such irregularities before; he knows they are usually reconciled in proper fashion at some later time. This time, however, a customer auditor is due shortly and he expects an NRC audit inspection imminently. If he had "time," he could straighten it all out, but there is no time. The expected visit from the outside cannot easily be postponed. His answer: to "specially" prepare for the audits; survive them; and go back and take care of the records later.

Buying time, in this case, has meant surviving an audit that the adversary is sure could be passed with no problem if more time were available. Other events linked to buying time are passing inspections, reconciling physical inventory, reporting acceptable MUF. In all cases, the motive is to alter just a bit of the troubled present in order to buy an immediate future that is troublefree, in the hope that with more time, proper adjustments can be made.

Buying time is subversive of Safeguards systems in three respects. First, any alteration in the representation of records or measurements directly weakens the capability of Safeguards systems to achieve the desired levels of accuracy and accountability. Second, intended later adjustments are quite often more difficult to accomplish than an adversary may believe when he makes the first fateful alterations. In fact, the extra time purchased by a misrepresentation may oblige the adversary to undertake additional wrongful acts in continual "adjustment" for the initial adversary action. Thus, a short-term objective becomes extended into a long range adversary sequence. Third, buying time --- once successfully accomplished --- teaches the adversary how to safely subvert the system. Since it was successful, he may consider invoking that remedy whenever discrepancies arise, rather than making the proper and required inquiries.

What motivates an otherwise diligent employee or group of employees to buy time? In the first instance, such an adversary must have some notion that by doing so "normal" resolution of difficulties will have the opportunity (i.e., the time) to take place. That is his rationalization. He may say to himself, for example, "If I hadn't taken care of things, a whole lot of hoopla over nothing would have occurred . . . but I took care of it and now everything's back as it should be." At the same time that the adversary rationalizes his acts as mere insurance that resolution will occur, he must also have a strong perception that an accurate reporting of difficulties would be unpleasant indeed.

Once an adversary acts to buy time, many of the ground rules change or intensify. Thus, the rationalization no longer is solely to allow resolution to occur but rather to conceal discovery of the original adversary act. Similarly, the perceived unpleasantry attached to the initial situation is magnified (and justifiably so) by the negative consequences likely to flow from a discovery not only of the original discrepancy but also of the adversary act which obscured its existence in the first place.

It is at this point that the characteristics of the adversary or members of the adversary combine become important. The more disciplined and controlled adversary will assess his detection vulnerabilities, will limit the number of adversary acts performed, and strategically, (i.e., very selectively) invoke his new-found power. A less controlled adversary, on the other hand, will come to define more and more situations as "needing time to get worked out." His acts will multiply, making the sequence top heavy and more readily detectable.

(b) To protect the license. Closely related to the motive to buy time is the motive to protect the operating license of a facility. Protecting the license, however, is generally a motive set in a longer time frame.

In simplest terms, "protecting the license" is a defensive posture with the overriding purpose being to keep operating --- no matter what the cost. From the perspective of those with this motivation, the best way to keep operating is to obscure --- insofar as is possible --- either the existence or the true dimensions of Safeguards problems or difficulties. Protecting the license, then, involves presenting to NRC, and customers, as stable and consistent a picture of smooth and troublefree operation as possible, regardless of current operational realities.

The defensive nature of the motive to protect the license may first emerge in the initial process of securing the license. Internal and external pressures related to plant construction, planned safety and health procedures, and Safeguards requirements may have resulted in protracted negotiation before license approval was received. "Getting operational" may have been costly enough that "keeping operational" --- at any cost --- becomes the best hope of recouping or offsetting start-up expense.

Defensive coloration of the true picture of things, then, may begin in the pre-license stage (in the falsification of construction or health-safety certifications, for example) or may emerge in reaction to pre-license difficulties after operations begin.[29] In either case, it will result in a posture which seeks to keep problems "in the family" regardless of the inherent danger such a stance presents to Safeguards or other NRC regulatory structures. Like buying time, the motive to protect the license may be easily rationalized as mere lack of candor rather than being viewed as actual fraud or misrepresentation, despite the fact that very real misrepresentations, failure to report accurately, or omissions in reporting are likely to occur. The adversary bent on protecting the license may satisfy himself that the slight adjustments he makes are really in everyone's best interest (i.e., jobs secured, power generated, economic growth sustained) and do not represent any real jeopardy to anyone.

The adversary may convince himself or themselves that he or they would definitely stop short of pursuing conduct with clearly injurious consequences. For example, suppose a contractor is found to have used relatively inferior materials for a basic construction task related to Safeguards protection. The error and liability would lie with the contractor, but exposing the discovery would also cost the licensee precious time, anguish, and money. In addition, the material used might not be truly inferior (it might have a stress strength, for example, that while adequate is less than that required by regulation). Given this situation, the adversary sufficiently

---

[29]Witness recent investigations into the falsification of X-rays showing pipeline welds on the Alyeska Pipeline Project. See, for example, New York Times, December 15, 1976, at p. A-19.

possessed of a system-generated protective motive may deduce that what is best for all is to attest to a falsified stress strength of the materials used by the contractor.[30]

(c) Protecting the organization or nuclear component thereof. The motive to protect the organization is one differing only in degree from the motive protective of the operating license. Conceptually, protecting the license may be seen as a logical offshoot of the concern for protecting the organization. Like license protection, this motivation is characterized by a defensive stance in which the health, well-being and investment interests of the larger business entity or instrumentality might be put above adherence to Safeguards requirements in operating licensee components. Protecting the license, for example, may emerge directly from a desire to make good on the prior investment of the larger organization for pre-license expenditures that were unanticipated. In this case, the objectives stemming from these two motives become substantially similar as their purposes intertwine. Alternatively, protecting the organization may reflect a conflict between the nuclear component and other divisions of the larger organization in competition for further corporate resources and continued investment commitments.

In any case, the protection of the organization and/or its nuclear component represents an attempt to secure a general future of stable operation free from disruption or outside intervention. Securing this objective may mean the submerging or misrepresentation of problems, failure to report or report accurately, or other acts subversive of Safeguards, safety or other requirements. The same rationalizations described earlier with respect to protecting the license are likely to be invoked with the same dangerous conclusion: "Under the circumstances, what I'm (or we're) doing really can't hurt anybody" --- a conclusion which whether fact or fiction is really not the point at all. These motives represent significant threats to Safeguards authorities when singlemindedly pursued by the white-collar adversary, even though they are defensive in character.

Undoubtedly the single most significant threat of these protective motives is their violation of the fundamental principle of a Safeguards system, that there must be accurate and full accountability for materials (and records thereof) entrusted to the care and custody of the licensee. Second, protective motives serve to create the need and provide the justification for developing ways of subverting or exploiting Safeguards systems. By doing so, they also generate fertile situations in which conduct adverse

---

[30]Such a white-collar crime may leave the facility vulnerable not to further white-collar threats, but to direct assaults on the weakened structure. Thus, white-collar adversary acts may create vulnerabilities to more conventional criminal threats.

to Safeguards goals can be learned and replicated (and in which assistance can be more easily recruited, if necessary). Such defensive motives, when more widely shared by adversary and non-adversary alike, may even subtly reinforce adversary conduct that is performed successfully, through praise received by those whose peers suspect them of manipulation. Third, Safeguards are vulnerable to the protective motives of the white-collar adversary to the extent that technical or letter compliance with regulations is emphasized. Finally, single-minded pursuit of the motives to protect the license or the organization may give rise to the specific threat represented in what we shall call the "good manager adversary."

The qualities that go into making a good manager also serve to make the good-manager-turned-bad a formidable adversary. A system-generated, defensive posture to protect the license or the organization would usually mean quick response and the use of countermeasures to prevent relevant external sources from learning of emergent problems. Carried to their logical extreme, these protective motives counsel not only quick response but conscientious anticipation of problems and contingency planning. This is where the "good manager adversary" enters.

The good manager is one who stays on top of the situation, entity or operation for which he is responsible; who maintains close contact with his subordinates in order to keep aware of how things are going; and who, should any problems arise, has careful back-up procedures or policies to counter or correct them. The "good manager adversary" has similar qualities except that his contingency planning is less bounded in that it permits consideration of wrongful acts in anticipation of potential problems. Set against the backdrop of an overriding concern for license or organization protection, the defensive posture of these motives becomes translated into the taking of affirmative steps not in response to but in anticipation of future problems. The "good manager adversary," then, may misrepresent, falsify, or alter not because he has a problem but *in case* he has a problem. His motive to protect means to avoid difficulties by prior adversary acts that will provide a buffer between his organization and relevant outside observers. This may mean squirreling away quantities of nuclear materials in anticipation of MUF problems; it may mean manipulating waste or MUF reports to create an illusory baseline for expected limits of errors; or it may mean reporting losses that have not occurred or vice versa.[31]

More troublesome is the possibility that the system itself or the organization may reward him for his activities. He may be known as the good manager, the man who looks ahead and is never caught by surprise. Distinguishing the good manager from the "good manager adversary" is likely to be extremely difficult --- particularly where problem avoidance is more

---

[31]It is the "good manager adversary" who is most likely to "test" the Safeguards system as described earlier at p. IV-6.

highly regarded than capable problem solving. But the "good manager adversary" may also be indistinguishable from his white-collar adversary counterparts responding to the same motivational structure. The difference between adversary acts taken to secure the future and those taken to insure against it, is likely to be subtle, but nonetheless important. And although the "good manager" may take comfort from the same rationalizations as other protective white-collar adversaries, his acts will be more affirmative than defensive in nature.

(d) To advance the organization. The motive of advancing the organization is more likely to be a part of the future than of the present civilian nuclear industry. It is also more likely to be found on a transnational scale, involving international as well as domestic Safeguards system violations. The two are not unrelated. The potential threat that an adversary may disregard domestic Safeguards in the interest of securing or protecting business interests may be easily translated to the international arena where Safeguards protections may be weaker and customers less averse to providing conspiratorial assistance --- or where customers themselves generate demands for white-collar acts.

The reality of a nuclear world in the next two decades is one in which there will be intense and increasing competition to supply technology, fuel and equipment. Such competition will exist not only among American nuclear companies but among them and their foreign counterparts. This competition will be bounded on one level by a set of IAEA Safeguards to which all or most parties will presumably subscribe. At another level, there may be further restrictions on supplier-competitors which emerge from individual treaty agreements made between supplier and customer nation states.

In such an international nuclear economy, where does the competitive edge lie? In superior technology and equipment? To be sure. In regularity and quality of fuel supply? Certainly. But the edge may also lie in minimization of the restrictions for customer utilization of materials and technology and/or the capacity to provide something unique --- unique because it is violative of restrictions placed on all competitors. It is here that the same rationalizations adopted at the facility level may easily be transferred to the international arena.[32]

(e) System-generated motives and related adversary objectives. Table 1 below presents a summary of the system-generated motives of the white-collar adversary described above, together with a listing of adversary objectives relevant to each motive.

---

[32]It should also be noted that learning how to violate international Safeguards protections may be instructive for a domestic diversion or violation.

TABLE I

SYSTEM-GENERATED MOTIVATIONAL STRUCTURES AND RELATED OBJECTIVES OF THE WHITE-COLLAR ADVERSARY

SYSTEM MOTIVATIONS	Related Adversary Objectives
Buy Time	to survive inspection where current data not credible to investigate discrepancies to cover up short run unexpected imbalances
Protect the License	to cover up large MUF to avoid regulatory interference over "minor" details
Protect the Organization	to protect financial investment to cover up suspected non-compliance affecting operation to avoid regulatory problems over discovered discrepancies
Advance the Organization	to assure continued market for organization to avoid international Safeguards requirements to exceed export limitations to undercut competitors in foreign and domestic markets

2. Position-Generated Motivations of the White-Collar Adversary. Motivational structures that can be viewed as position-generated parallel, to a large extent, the system-generated motives described in the preceding sections. They are, in effect, individualized interpretations of substantially the same pressures for accuracy and accountability that affect system-motivated acts. The difference is really one of emphasis. The system-motivated white-collar adversary, for example, responds in terms of a defensive or insulating concern for his facility or organization, a concern which derivatively is self-protective as well. The position-motivated white-collar adversary on the other hand seeks self-protection as a first priority, from which derivative protective benefits may accrue to his firm or organization but these are not his primary concern. This adversary may reach his greatest potential where objectives promoting his self-interest coincide with those protective of his organization, but where choices must be made, he will seek self-protection before a more generalized defense of his firm, fellow employees or industry.

The distinction between the system-motivated and the position-motivated adversary is not an easy one to make. To begin with, the conduct of the white-collar adversary in both cases will appear strikingly similar, and the consequences of the conduct may well be the same. In addition, the two motivational structures are likely to be significantly interdependent. Thus, a system-motivated white-collar adversary may depend for success on his ability to recruit adversary partners who have a selfish interest in contributing to a scheme which the initiating adversary "unselfishly" conceived. Alternatively, those involved in what initially was system-motivated adversary conduct may develop strong self-protection motives as a result. Over time, concern for the organization may give way to concern for insulating oneself should the larger scheme be discovered.

One distinction not likely to be relevant to the issue of system versus position-generated motivations should be noted at the outset, and that is the level of position held by the potential white-collar adversary. It may be tempting to suggest, for example, that vice-presidents may be system-motivated while loading dock foremen are not. But job classification is not a good predictor of motivational structure. Lower level production personnel and managers may have a far more developed sense of "company loyalty" than high level managers whose professional skills and competence may be attractive to a variety of employers. Alternatively, the possibility of rapid and significant professional advancement may be more likely for middle and upper level personnel than for their subordinates, making the stakes and need for self-protection greater than those which exist at less promotion-oriented employment levels. Nevertheless, those in high level positions may possess a vantage point from which the longer range goals of system-motivated adversary conduct can be conceptualized, identified with, and justified --- a perspective potentially lacking in many lower level positions. The point is that one's job does not necessarily determine the category of motivation to which he or she responds.

So long as personal and organizational ends remain essentially identical, distinctions between the system- and position-generated motivations of the white-collar adversary are likely to be very small. They will not always remain the same, however, and it is both the points at which they separate *and* the ways in which they are mutually dependent that become significant subjects for discussion. The three position-generated motives presented below, then, focus on these points of separation and interdependence rather than on general description.

(a) Buying time. The position-generated motive to buy time has the same short run objectives as its system-generated counterpart. To some extent the position-motivated white-collar adversary may not be totally selfish in an attempt to buy time. He may want to protect his immediate supervisor(s) or subordinates as well as himself. The important difference between him and his system-motivated counterpart is in his focus. He will tend to be more personally or section-oriented rather than to have facility-wide or organizationally bounded perspectives. His interpretation of danger or unpleasant consequences, therefore, may be quite narrow in scope, and his adversary acts in defending against such consequences may similarly be narrowly drawn.

While the position-motivated white-collar adversary who buys time has the advantages of rationalizations and justifications similar to those of his system-motivated counterpart, he also has the same problems. Going back to make the intended adjustments may prove more difficult and more risky than it seemed initially. Setting the record straight may involve further adversary acts or prove too vulnerable to detection to be accomplished. Both of these situations put this adversary in an unanticipated bind, but his response in each case may be different.

If the position-motivated adversary finds that further acts are necessary to his buying time, or subsequent cover up, he may very well continue his adversary sequence beyond that originally planned. Where detection due to readjustment is perceived as too risky, however, he is more likely to avoid readjustment acts. His refusal to expose himself to a high risk of detection in making a later readjustment may expose the organization but it is a chance he may take. If he is successful in this situation, what the position-motivated, white-collar adversary will have done is to buy time successfully, but by failing to make a later readjustment, he will also have created a permanent false record on which his organization and others outside it may rely. Had the risks of personal detection been smaller, he would have made a subsequent readjustment to correct the record. It is in this sort of situation that the priorities of the position-motivated adversary will make his conduct different from that of his system-motivated counterpart.

(b) To cover up past error. Whereas the motive to buy time (under either the position- or system-generated structure) represents an adversary response to real-time or current errors and discrepancies, the motive to

cover up past error is a response to discovery of problems of long standing. Characteristic of the type of situation in which this motive might emerge would be one in which an employee or supervisor of a section of a facility (an MCA or QC area, for example) discovers in the course of work that a repetitious and unintentional error, systematic in nature, has been made over time. Previously unknown, the error has been applied to all operations (measurements, etc.) performed by the section. Such an error is no one's fault really and does not represent any wrongdoing. It may in fact be based on a machine or calibration failure.

In a system-motivated framework, such a discovery is quite likely to be reported and thus not generate an adversary sequence. This is because recalibration or whatever is needed may have positive long run consequences for the organization as would the demonstrated internal vigilance of the facility. Where the position-motivated discoverer is concerned, however, the issue may not be so clearly seen and the probability of a non-adversary response becomes less likely. Thus, without the benefit of a larger perspective, the employee or employees in a particular section of a facility may see more negative than positive consequences accruing from a report of the error. The failure to discover the problem sooner may weigh more heavily on the white-collar adversary in this instance than the importance of the discovery. He may interpret the discovered error as reflecting on his job performance, i.e., because he was capable of discovering it now, he should have uncovered it sooner.

Because this potential adversary both views and interprets events from such a confined and myopic posture (i.e., as they relate to himself), the cues he may take from situations may suggest the adversary-like path as the best course of action. In this case, covering up the discovery will cover up the error. Particularly susceptible to this adversary motive is the individual seeking promotion either to a managerial position or within managerial ranks. Because advancement is his consuming interest, he will be more likely to interpret such a discovery as a threat to advancement than as a benefit. He may convince himself that it will be held against him when review for promotion is made.

Once the adversary objective of obscuring the error discovery is set, this adversary has one further problem: how to proceed in the future? The path of least resistance would be to ignore the discovery entirely, and proceed as if nothing had occurred. The problem with this is that he may begin to feel some guilt (i.e., he may be forced to view himself as something of an adversary). This is a critical situation; the white-collar adversary handles himself best, accomplishes most, and finds recruiting others easiest when he can "justify" his conduct and avoid any thought of its wrongful nature.

Another course of action open to the position-motivated adversary is to begin making small adjustments toward what he knows to be a truer representation of the status of nuclear materials at his station. So long as the adjustments are minor enough, it may be possible to accomplish this without causing problems throughout the entire facility. The risks here are somewhat greater than complete coverup would be, but his conscience may be much eased by the rationalization that he is moving toward honest reporting. This in turn may make it easier to accomplish his acts and/or to recruit others to assist him. The attempt to recruit others may be propitious from a Safeguards perspective because it may provide the adversary with other viewpoints. This may cause him to interpret the discovered error in a less egocentric fashion, to weigh the positive consequences of reporting his findings, and to retreat from an adversary path. At the same time, however, recruitment of others discloses to them that adversary acts are both contemplated and planned within the facility --- a disclosure that may motivate them to become white-collar adversaries on their own under other circumstances.

(c) To advance professionally. Whereas the previous two position-generated motives involve adversary responses to present or past problems, largely self-protective in nature, the professional advancement motive is almost totally egocentric. An adversary influenced significantly by his ambitions will tend to evaluate all issues in relationship to those ambitions. Thus, problems or discrepancies of little consequence to the organization or facility can have (or be interpreted to have) great consequence for him. This is because he sees himself as precariously poised in the organization --- either he has or is about to rise meteorically or he feels in danger of losing his position. This adversary believes he can afford nothing short of a trouble-free record.

The white-collar adversary acting in response to this motive may have a special ability to enlist assistance. Subordinates or fellow employees may see their futures hitched to his. They may also be easily persuaded that the organization itself condones the questionable activity in which they are asked to participate, i.e., that's the way people "make it" around here. This adversary may also shroud his egocentric motives in an appeal for company loyalty. The higher the position of such an adversary, the more people he will be able to influence, the more credible his message will seem, and the more his personal motives will be taken as representative of the organization's best interest.

(d) Position-generated motives and related adversary objectives. Table 2 below presents a summary of the position-generated motives of the white-collar adversary, together with a listing of adversary objectives relevant to each.

(e) Interdependence of motivational structures. The most significant threat to Safeguards which could flow from system- and position-generated white-collar motivational structures would be the education they provide the

TABLE II

POSITION-GENERATED MOTIVES AND RELATED OBJECTIVES OF THE WHITE-COLLAR ADVERSARY

POSITION MOTIVATIONS	Related Adversary Objectives
Buy Time	to investigate discrepancies in section operation to cover up short run unexpected problems to avoid being cause of facility problems with NRC
Cover Up Past Error	to avoid report of discovered error to prevent poor personal evaluation to avoid causing organizational problems with NRC to assure promotion
Professional Advancement	to cover up problems that might affect personal achievement to portray a perfect management record showing no section problems to avoid reporting discrepancies

potential adversary. What each set of motives presents are situations in which this adversary can learn to create adversary sequences and pursue adversary objectives, possessed of a self-righteousness and of the conviction that he really is not an adversary at all. Such motives come complete with convenient rationalizations (i.e., "I'm protecting the company"; or "why cause problems over nothing") and justifications for manipulation of Safeguards rules and regulations (i.e., no real harm will be done). At the same time that the adversary is learning specific kinds of conduct, however, he can "learn" disregard for Safeguards authority and objectives.

Learned manipulation and deception of Safeguards systems in settings replete with *apparent* justification can potentially be transferred to situations where no such rationale or justification could possibly exist. Similarly, acquired disregard for Safeguards learned from successful manipulation "for good cause" removes a final inhibition to conduct which the white-collar adversary will himself recognize as adversarial in nature. We turn next to this arena, the individually-generated motivational structure of the white-collar adversary.

3. Individually-Generated Motivational Structures. Motives of the white-collar adversary that are individually-generated are somewhat easier to conceptualize than are system- or position-generated motives, but often far harder to understand. Individualized motives differ from other motivational structures in two important respects. First, because they are not tied to organizational goals or ends the earlier described rationalizations and justifications are absent. Second, without the same rationalizations it is difficult for the white-collar adversary to maintain the view that his conduct is "innocent" or "harmless" in nature. In this regard, individually-derived motives are likely to be powerful ones since they involve conscious subversion of the system(s) by which the adversary is employed and in which he enjoys a trusted status.

Individualized motives generate white-collar adversary sequences that serve the adversary's own ends rather than his employer's or firm's purpose. As noted earlier, the process by which the white-collar adversary learns subversive conduct may shape his pursuit of such conduct for personal ends. Thus, while the acts of an individually-motivated adversary are not supported by the same rationalizations as those of the system- or position-motivated adversary, they will not be devoid of justification from the adversary's point of view. If the adversary has learned manipulative conduct as part of a system- or position-oriented adversary group, he may be motivated to free-lance for his own benefit. Similarly where this adversary has seen his organization or his supervisors violate their positions of trust, he may see little wrong with his doing the same. This is why the climate of an organization's overall compliance with Safeguards requirements becomes tremendously significant in assessing the potential of the white-collar threat in that organization.

Four separate individually-generated motives are discussed below. While all four are equally threatening to Safeguards objectives, the potential harm resulting from each is likely to differ. As each is discussed, then, attention will be given to the relative harm engendered in connection with it.

(a) Intellectual game-playing. The intellectual game-player is the one individually-motivated white-collar adversary least likely to view himself as such, although he cannot help but realize that he is subversive of the system in which he works. However, because his real objective is to test his own mental prowess against that of the Safeguards system he will understand the challenge he presents to that system but will not necessarily see himself as making it vulnerable. Rather, he will be demeaning it in his own eyes. What makes highly intelligent, trusted employees toy with sophisticated control systems in which they work is difficult to determine but examples of such game-playing have been found in many complicated public and private areas of activity. In this respect, the game player, though likely to be extremely rare, is an adversary who cannot be totally ignored.

The game player adversary has no real motive to steal or divert nuclear material. He merely wants to see how far one can go "hypothetically," using his wits to defeat the system. Often highly intelligent, he enjoys reaffirming just how bright he really is --- even though he may feel that those around him don't truly appreciate his genius. He may convince himself that when and if he finds a significant weakness in the system he will bring it to the attention of the proper authorities. When that time comes, however, he is likely to realize --- quite rightly --- that his unrequested black-hatting of the system is less apt to meet with congratulation than with censure. Reporting of the discovered weakness, then, will not occur and the information will be stored in his own head for self-satisfaction and perhaps future reference.[33]

The game-player manipulates the system, then, for what is a hypothetical purpose. That is not to say that he will not internally divert nuclear material and/or alter records, and thus commit affirmative adversary acts. Though his purpose is wrongful, he will consider it theoretical, i.e., to see if it can be done, rather than to cause harm or put the system at risk. His adversary acts, though theoretical from his perspective, however, will both harm and risk the Safeguards system. For if he can learn to manipulate it successfully, he may increase the system's vulnerability.

(b) Avenging a perceived wrong. The motive of revenge may occur whenever an employee has a real or perceived grievance against his employer or the system in which he operates. This is a common motive for sabotage in

---

[33]Such as his acquiring a different motive.

industry generally, and there is no reason to doubt that such sabotage in the nuclear industry could take the form of white-collar adversary acts. The adversary in this situation may not think through the consequences of his conduct, which makes the potential harm both dangerous and largely unforseen by the adversary until perhaps too late.

Generally, the vengeful white-collar adversary will have a high concern for self-preservation and will not seek objectives which will personally jeopardize his position. On the other hand, he will have little concern for protecting the organization and may purposely put it in jeopardy so long as he can remain unidentified. Because the individually-generated motive to avenge a perceived wrong is so powerful, this adversary is extremely dangerous. His potential for serious harm is great, mostly because he will give the consequences of his acts little thought. Revenge for its own sake will blind him to the more general risks he creates that go beyond the target(s) of his displeasure. Though intending harm to his employer but not to his general community, he may find only too late that he has created a serious community risk.

(c) The motive to extort. The white-collar extortionist will have little difficulty in conceiving of himself as an adversary. The motive to extort may arise out of either of the two motives described above, or may derive from the objective to acquire some monetary, psychological or political advantage. The successful extortionist must at some point be a good game-player, and his decision to extort may have been preceded by previous theoretical "tests" of the Safeguards systems.

The white-collar extortionist represents a greater threat than other extortion adversaries because he will have access to both inside information and (perhaps) nuclear material or records to make his threats particularly credible. The white-collar adversary is less likely to actually divert or steal material to back up an extortion threat than to create the appearance that a significant amount of material is missing and unaccounted for. If he diverts material at all it will be to secrete it in the facility rather than to carry it away. This is because it is not material he wants, but money, system confusion, fear, or some combination thereof.

Even though the white-collar extorter will have insider knowledge he will use it sparingly and will strive to avoid the use of information which might specifically identify him. He will, however, be sufficiently knowledgeable to employ information which will give credence to his threat but not be traceable to him.

(d) The motive to sell nuclear material for financial gain. The selling of nuclear material for personal gain is more likely to be a credible hazard in the future than at present. The development of an international nuclear economy may create both licit and illicit market structures and

mechanisms to which both organizations *and* individuals may relate. In any case the potential for realization of financial advantage from the theft and sale of nuclear material and process products represents a significant challenge to nuclear Safeguards authorities which has been considered but not yet been the subject of systematic in-depth study.

An illicit market in which stolen nuclear material and products can acquire commercial value challenges Safeguards systems on two levels. First, it requires Safeguards authorities to anticipate its evolution and development, and the general threats thereby created. Second, it challenges Safeguards authorities to also anticipate its specific characteristics and dimensions in order to know the relative values such a market will place on different nuclear materials, and how these valuations are established. The latter challenge may require new Safeguards definitions of material attractiveness and vulnerability. While the motive to achieve monetary gain from nuclear theft may be a future one, the potential complexity of the arena(s) in which it may be satisfied requires current concern and planning.

An important subset of the motive to sell nuclear material for monetary gain involves the situation in which such a motive may be instrumental in solving a personal problem. White-collar crimes are frequently committed outside the nuclear area in order to solve short and long-range personal financial problems. Often the ultimate monetary gain from such theft accrues not to the adversary but to another to whom he is obligated in some way, e.g., loansharks, gambling creditors, etc. While the adversary stealing for his own advantage is likely to perform continuous, repetitive acts to acquire valuable material,[34] the white-collar adversary stealing to ease or eliminate a financial burden is more likely to cease adversary acts once the burden has been removed. The capacity of this adversary to stop depends, of course, on the nature of his personal problem. Two general classes of financial problems can be described. The first of these is the debt derived from tragic or unfortunate personal situations, e.g., the deteriorating health of a family member. Often such debts can assume tremendous proportions incapable of traditional solution where an employee is already over-committed financially. A study of simple embezzlement by Cressey[35] found a significant class of employee-embezzlers motivated by such difficulties which they considered "unsharable personal problems." A white-collar adversary in this type of situation will have a particular monetary goal in mind and plan an adversary sequence to continue until that goal is reached. This will make him a highly-motivated but less-than-totally-committed adversary, whose subversive acts create considerable personal internal conflict. For this reason, he may be more detectable than other white-collar adversaries.

---

[34]Using current definitions, a sequence would generate amounts of material so small as to seem valueless, but current definitions may not determine the needs of a possible future illicit market which might combine supplies from numerous sources, or have customers with special and unique requirements.

[35]Donald B. Cressey, Other People's Money: A Study in the Social Psychology of Embezzlement, (Glencoe, Ill.: Free Press, 1953).

The other class of financial problems to which the white-collar thief may respond involves indebtedness related to personal vices or abuses, such as gambling, loan-sharking, etc. This type of problem is not as well-bounded as the first type since the "solution" creates its own problems. The adversary obligated to a loan shark, for example, is not likely to have a clear picture of the total amount of money he needs and will find extrication from indebtedness an ever-receding target. This will make it difficult for him to bound his adversary sequence. These kinds of obligations also make the adversary extremely vulnerable to blackmail and extortion, forcing continuation of adversary acts beyond the point at which the original obligation is satisfied.[36] In this case, the adversary is really working for others from whom he may receive direction and potentially even assistance in performing subversive conduct. His "job" may require him to merely supply shipping or security information to his new "bosses" or to engage directly in covert thefts.[37]

Those with "unsharable personal problems" are most likely to operate alone. All other individually-derived motives are capable of generating adversary combines for successful achievement of objectives. The personal financial motive, however, will tend to isolate the individual adversary. This may make this adversary less of a threat than others unless the outsiders pressuring him can provide significant assistance to substitute for the lack of insider-partners.

(e) Individually-generated motives and related adversary objectives. Table 3 below presents a summary of the individually-generated motives of the white-collar adversary, together with a listing of adversary objectives relevant to each.

C. WHITE-COLLAR IMPLEMENTING ACTS AND ACTIONS

White-collar adversaries will differ from each other with respect to their capacity to access attractive material or records and their susceptibility to and probability of detection, i.e., their opportunities for accomplishing adversary sequences, as well as the motivational structures and specific objectives to which they relate. However, when one considers the implementing acts or actions in support of the white-collar adversary's objectives, commonalities among diverse white-collar adversaries emerge.

---

[36]The same may be true to some extent of adversaries who, for different motives, sell stolen material illicitly.

[37]Situations like these have been found by numerous investigative groups concerned with cargo theft and security issues.

TABLE III

INDIVIDUALLY-GENERATED MOTIVES AND RELATED OBJECTIVES OF THE WHITE-COLLAR ADVERSARY

INDIVIDUAL MOTIVATIONS	Related Adversary Objectives
Intellectual Game-Playing	to test the "intelligence" of the system to see if small amounts of material can be diverted
Revenge	to cause alarm over unexpected losses to sabotage a facility's good record to produce record and/or material imbalances to create internal and external (NRC) suspicion and concern
Extortion	to acquire financial, psychological or other advantage via a credible threat
Sell Material for Financial Gain	to acquire salable amounts of attractive nuclear material to acquire requisite amounts of salable nuclear material to satisfy debt to answer blackmail or extortion demands with material and/or classified information

These commonalities among the implementing acts of diverse white-collar adversaries derive first from some inherent qualities of these acts regardless of the purpose(s) for which they are undertaken; and second, from the complexity of the system(s) in which the white-collar adversary might operate. The commonalities are their (1) subtlety; (2) clandestine nature; and (3) complexity. The following discussion focuses on each of these common qualities.

1. The Subtlety of White-Collar Adversary Acts. Unlike the acts of adversaries considered by most studies of the Safeguards systems, implementing acts of the white-collar adversary are not likely to be direct and overtly inappropriate in nature. White-collar acts are likely to conform as closely as possible to "business as usual" or "standard operating practices." The reason for this is that the white-collar adversary seeks to cloak his acts in a facade of legitimacy that can mask their true character (i.e., the *disguise* element noted earlier).[38] Only in this way can he be truly successful.

What this will mean is that the acts of the white-collar adversary will usually comport with his proper area and scope of authority, i.e., will be within the scope of his normal work activity or within the work activity of another whom he knows well and can successfully, though falsely, represent. The range of subversive acts that the white-collar adversary can subtly and successfully perform will be determined to a large extent by his job-related characteristics, i.e., his degree of access to attractive material and information (pp. IV-3ff). The adversary may enlarge his scope of possible acts or actions by the contributions of co-conspirators who might be recruited to assist him. Adversary partners can bring not only their own job-related qualities, but also a wider range of authority that can be misrepresented successfully. Thus an adversary who must alter internal transfer documents in order to accomplish a particular objective will find it much easier if, as one signatory, he can enlist the aid of the second necessary signatory (or one capable of falsely representing that signatory) to such a transfer document.

The capacity to recruit a co-conspirator successfully will depend not only on personal attributes such as persuasiveness, but also on the degree to which the adversary's motive and objectives can be adopted by a potential recruit. Thus, system-motivations may be more salable to potential co-conspirators than are individual motivations. In any case, addition of adversary partners will enlarge the range of acts that while subversive in nature can comport or seem to comport with proper conduct.

Subtlety of implementing acts is important to the white-collar adversary for two reasons. First, subtle acts allow the adversary's true purposes to remain disguised. An intended diversion of nuclear material, for example, is better disguised through the preparation of artfully

---

[38]See p. III-3 ff.

contrived transfer documents than by an attempt to carry it from a facility (past a detection device) on one's person. Second, acts that are subtle in nature will not immediately raise internal alarms as overtly improper activities might. Instead, the white-collar adversary will appear to be "doing" what "he always does" and in a fashion entirely consistent with anticipated conduct. The more meticulous and subtle the act, the more significant is the white-collar adversary's threat and potential success.[39]

A Safeguards' emphasis on procedure may not be the best response to the white-collar adversary, for this adversary will attempt to act in total adherence to procedure. If double signatures are needed, he will have them. Where authentication is necessary, he will supply it. As much as is possible, the implementing acts of this adversary will be devoid of any overt adversary character. It will be "business as usual," only the business he represents is likely to be totally or partially false.

2. The Clandestine Nature of White-Collar Adversary Acts. Clandestine nature is a second common characteristic of the acts of the white-collar adversary, setting him apart from other adversaries who desire merely to effectively complete an action sequence. The inherent success of the white-collar adversary depends either upon his implementing acts not being detected, upon their being misinterpreted, or upon their being discovered so long after their occurrence as to be untraceable to him. The clandestine quality of acts is, of course, not unrelated to subtlety. Thus, the more this adversary's acts comport with proper and customary practice, the more likely they are to remain clandestine and hence concealed from detection. Within each white-collar implementing act is implied one of three characteristics:

- that the act itself is inherently undetectable;
- that the act will be followed by an act(s) of cover-up that will make detection difficult; and/or
- that detection of the act will be delayed long enough so that "reasonable" explanations supplied either by the system or the adversary himself will account for apparent discrepancies either in records, procedures, material location, or quantities of nuclear materials on hand.

(a) Inherently undetectable acts. Practically speaking, few if any acts are totally undetectable given infinite monitoring resources. "Undetectable" in this sense, then, does not connote true impossibility of

---

[39]This dimension of subtlety assists the white-collar adversary in both concealment and in achieving the necessary voluntary system assistance he needs to achieve his wrongful purpose.

detection but rather a remoteness of detection possibility given a rational level of surveillance in Safeguards systems, e.g., one which bears a reasonable relationship to costs, burdens of nuclear industry operations, and contemporary assessment of the level of the threat. The white-collar adversary will assess the relative probabilities of detection of a given set of acts and obviously opt for those having the least potential for detection. In evaluating a range of acts possessing equal degrees of subtlety, the following is likely to be true:

1. Acts of omission will be relatively less detectable than acts of commission.

2. Acts whose successful performance is confined within a section of a facility will be relatively less susceptible to detection than those actions which must be performed across section or facility boundaries.

3. Acts that can be performed totally within the adversary's legitimate scope of authority and responsibility will be relatively less detectable than those requiring the additional authority of others.

4. Acts that can be cranked into the system as baseline data (i.e., that involve data or records totally controlled by the adversary or adversary group from origination through authentication and verification) are significantly less detectable than those subject to redundant checks not under such control.

(b) Cover-up acts making detection difficult. Because few adversary acts are totally undetectable, the white-collar adversary is more likely to rely on cover-up acts for concealment of original adversary conduct. Cover-up acts can consist either of extended adversary action sequences or of repetitions of the original act. The extended adversary sequence is essentially an act that requires several steps that may be time-lagged in some fashion for concealment purposes. Thus, for example, falsification of records to reconcile measured and expected MUF might be followed by later alteration of waste records consistent with falsified MUF reports.

Acts that are repetitions of initial adversary conduct also serve concealment purposes. For example, diversion of a small amount of nuclear material, accomplished by the introduction of systematic measurement error, may be covered up by continued introduction of the same error. Thus, the diversion can only be detected if and when the systematic error is detected --- *and* recognized as purposeful error.

(c) Undetectability deriving from delayed system response. Acts that are neither undetectable nor capable of being successfully covered up can still be made clandestine by a lag in the detection time. The white-collar adversary may rely on the system itself to provide a delay in detection. In the example noted above regarding systematic error introduction, if detection of the error occurs long after its initiation, it may be impossible to link it to purposeful adversary conduct. Thus, such error may be attributed instead to measurement or calibration problems. Time lag in this situation might handicap detection of either the adversary content of the error *or* the objective it supported, e.g., diversion of small amounts of nuclear material.

Similarly, actual cross-checks and balances among redundant record keeping systems may occur less frequently than subsystem adjustments and corrections. Lags in posting such adjustments may be considered to account for balance discrepancies rather than acts of record alteration performed by the white-collar adversary. Often the system itself (or its managers), sufficiently convinced that nothing amiss has or could occur, may supply its (their) own reasons for discovered discrepancies.

3. Complexity of White-Collar Adversary Acts. In addition to being subtle and clandestine, the implementing acts of the white-collar adversary will tend to be complex. "Complex," in this context, refers to an intricacy of conception and planning and to the manner in which the implementing act will take effect, rather than the nature of the act itself, e.g., a single simple act such as a record alteration will have broad and complex ramifications as it impacts on different parts of the environment in which the record moves. Complexity is introduced by: (i) the extent to which acts are to be undertaken repetitively; and (ii) the closed system in which they must be executed. The relationship between repetitiveness and complexity is not always direct and positive. Rather, a one-time act may involve far more complex planning in order to be subtly and easily concealed than an act that is to be systematically repeated over time (where, for example, each replication of the act essentially "corrects" for the initial improper act). On the other hand, the more systematic and repetitive an adversary's acts, the more vulnerable their pattern is to potential observation and detection.

The complexity of the white-collar adversary's acts is further necessitated by the fact that he generally will operate in a closed system, i.e., a licensed nuclear facility. All input to such a facility must eventually be accounted for within measured limits as either output, inventory, waste, or MUF. Limits of error are narrowly drawn in ranges which, over time and per recorded measurement, must conform to established standards. There is very little "give" in the total system despite limitations on achieving precise measurement of most process and scrap material.

The white-collar adversary, then, is faced with rather strict constraints on his manipulative capacity, which complicate his tasks. However, these system constraints are a double-edged sword. For at the same time as standards for limits of error represent constraints on the white-collar adversary, they also serve as useful parameters against which to gauge the inherent riskiness or detectability of his acts. In this sense, established limits of error become for the white-collar adversary *limits of system tolerance*. If he can manage to operate within those limits, he can hope to remain "safe." The system will have provided him with needed guidelines for an "acceptable range" of improper acts, or alternatively with guidelines for the requisite cover-ups needed to conceal his conduct. Complexity introduced by the Safeguards system, then, can both hinder and serve the white-collar adversary.

D. MOTIVATIONAL STRUCTURES, OBJECTIVES AND POTENTIAL IMPLEMENTING ACTS OF THE WHITE-COLLAR ADVERSARY

Table 4 below reintroduces the motivational structures and related objectives of the white-collar adversary (presented earlier in Tables 1-3),[40] linking these to potential white-collar implementing acts supportive of such motives and objectives. Since a more complete listing of possible implementing acts would be very extensive, those included are intended to be representative of the kinds of acts the white-collar adversary might use. Implied within each act listed are the qualities of subtlety, clandestine nature, and complexity described in the preceding sections.

---

[40]See respectively pp. IV-20; IV-25; and IV-31.

TABLE IV

MOTIVATIONAL STRUCTURES, OBJECTIVES AND POTENTIAL IMPLEMENTING ACTS OF THE WHITE-COLLAR ADVERSARY

SYSTEM MOTIVATIONS	Related Adversary Objectives	Potential White-Collar Implementing Acts
Buy Time	to survive inspection where current data not credible	falsification of non-credible data
	to investigate discrepancies	alteration of records reporting suspect data
	to cover up short-run unexpected imbalances	falsification of balance records/reports
Protect the License	to cover up large MUF	under-reporting of MUF
	to avoid regulatory interference over "minor" details	falsification or alteration of records reflecting problems
	to keep operational	failure to report suspected loss or diversion
Protect the Organization	to protect financial investment	(same as above, plus): over-reporting of MUF or waste to acquire material cache
	to cover up suspected non-compliance affecting operation	manipulation of inventory counts or records
	to avoid regulatory problems over discovered discrepancies	
Advance the Organization	to assure continued markets for organization abroad	(same as above, plus): alteration of transport documents
	to avoid international safeguards requirements	failure to accurately report sales of material or equipment
POSITION MOTIVATIONS		
Buy Time	to investigate discrepancies in section operation	failure to report discrepancy
	to cover up short-run unexpected problems	falsification of discrepant section data
	to avoid being cause of facility problems with NRC	alteration of section reports
Cover Up Past Error	to avoid report of discovered error	(same as above, plus): continued application of systematic error
	to prevent poor personnel evaluation	falsified reporting of section material
	to avoid causing organization problems with NRC	
	to assure promotion	
Professional Advancement	to cover up problems that might affect personal advancement	(same as above, plus): manipulation of inventory or on-hand accounts and records
	to portray a perfect management record showing no section problems	acquisition of material cache
	to avoid reporting discrepancies	
INDIVIDUAL MOTIVATIONS		
Intellectual Game-Playing	to test the "intelligence" of the system	alteration of material records
	to see if small amounts of material can be diverted	falsification of documentation, authentication of originally generated data
		fraudulent transfer of material within facility to hiding place
Revenge	to cause alarm over unexpected losses	(same as above, plus): fraudulent internal movement of noticeable quantity of nuclear material
	to sabotage a facility's good record	record alteration and falsification to suggest non-compliance
	to produce record and/or material imbalances	
	to create internal and external (NRC) suspicion and concern	
Extortion	to acquire financial, psychological or other advantage via a credible threat	record and/or data falsification to create appearance of diversion
		fraudulent internal transfer to covert location
		diversion via fraudulent shipping or other documents
Sell Material for Financial Gain	to acquire salable amounts of attractive nuclear material	fraudulent external transfer of material
	to acquire requisite amounts of salable nuclear material	fraudulent alteration of documents authenticating external transfer
	to satisfy debt	alteration of documents, records and measurements to coincide with falsified transfer
	to answer blackmail or extortion demands with material and/or classified information	

V. REGULATORY COMPARISONS

The fact that regulation in the nuclear field evolved in a manner substantially different from that in most other regulatory areas[41] does not mean that this evolution took place without the benefit of other regulatory experience. Quite clearly much other regulatory experience found its way into this field through lateral staffing, and all of the normal interactions which are to be found in the Federal Government. Nevertheless, it should be helpful to make some comparisons between nuclear licensee regulation and other regulatory and administrative activity, since the ever-present pressures of coping with the complex nuclear field on a day-to-day basis may have tended to obscure some of the differences and similarities.

A. THE REGULATORY PLATFORM

The manner in which the civilian nuclear industry was established differs from that of most regulated industries, though the resemblance to NASA support of aircraft technology has been noted. Eads and Nelson made this point quite forcefully:

> During the 1950s and throughout the 1960s, the Atomic Energy Commission gradually increased the extent of its involvement in the development of civilian nuclear power, both in terms of detailed planning and subsidy of development, *and in terms of admonishing industry to do more than it seemed to want to do.*[42] (emphasis added)

Initial regulatory objectives thus included both technology promotion and strict and severe control of that same technology. This does not mean that the Federal Government was in any way a supplicant to industry, which had its own very substantial motives for cooperating in these technological developments, but the control relationship was clearly quite different from that found in financial or other regulatory fields where government surveillance focused primary on controlling industry activity. There is some partial analogy in some regulator-regulatee relationships where the financial health of an industry is an agency objective, or where the regulator actions help to determine day-to-day operational policies (as in the case of the relationship between the Federal Reserve System and our nation's banks). There are very real differences, however, between

---

[41] See Introduction, pp. I-4-6.

[42] George Eads and Richard R. Nelson, "Government Support of Advanced Civilian Technology: Power Reactors and the Supersonic Transport," Public Policy, at pp. 405 and 409; Phillip Mullenbach, Civilian Nuclear Power: Economic Issues and Policy Formation, (New York: Twentieth Century Fund, 1963).

encouraging more efficient and more profitable operations and trying to launch a new industry which will be regulated. This element in the relationship between regulator and regulatee must be regarded as an inhibiting factor with respect to implementing controls.

Two factors tend to offset this inhibiting factor in the civilian nuclear industry. First and most important, concerns about the dangers of diversion or theft of nuclear materials, and about safety of nuclear industry operations are regularly raised by members of the Congress, the media, and public interest groups. Second, there are now large numbers of licensees who have made massive investments in nuclear technology, and who have, in part, foregone the opportunity to meet their energy commitments to customers from other sources. The commitments of these licensees are, however, partially counterbalanced by genuine concerns as to how they can confidently plan for the future in light of ever-present public policy debates and heavy capital investments required by the nuclear energy production route.

It is possible that these opposite influences on the regulatory control tend to cancel each other out. This, however, would presuppose that all these forces are working at the same time. They may in fact be working sequentially rather than simultaneously, which raises the possibility that judgment calls on regulatory policy (as opposed to enforcement through monitoring and inspection) may occasionally give less weight to Safeguards considerations than at other times. This may be less of a problem with respect to protections against conventional threats which are more easily comprehended by all parties in interest than against white-collar adversaries who would tend to exploit more subtle system weaknesses and be more aware of such weaknesses.

B. THE INSTRUMENTS OF REGULATION

Safeguards controls are implemented through formally promulgated regulations, regulatory guides, inspection policies, licensee internal plans and procedures, and reference to licenses granted to specific private enterprises.

The operations of these private enterprises, the licensees, are highly complex and varied. Each facility (whether fuel fabricator, reactor, etc.) has its own very individual characteristics. Its license is in a very real sense an individually tailored instrument which incorporates a set of assumptions which constitute regulatory parameters for the NRC, as well as narrower inspection parameters for the NRC staff. This is in marked contrast to other regulatory structures. In other regulatory areas a license may be required as a condition of operation, but such a license is generally conditioned on showing (a) resources needed for the operation, generally financial, (b) capability and fitness of management, and/or

(c) public need for the services to be provided by the licensee. This is in contrast to the private nuclear industry, where the license stresses specifics of individual operating patterns, details of the construction of facilities peculiar to each licensee, and internal control mechanisms dealing with the manner in which it handles, moves, and secures its working inventories.

In other regulated industries, operations are likely to be monitored along general guidelines and not by reference to the individual licensee's own charter. In the private nuclear industry, NRC regulations will determine the conditions of the license, but the license will in turn control the manner in which the regulations and regulatory inspection mechanisms are invoked against the licensee.

C. RELEVANCE OF OTHER REGULATORY EXPERIENCE

The NRC pursues its Safeguards and other regulatory objectives from an initial interaction base quite different from that of other regulatory agencies, as noted above. Nevertheless, the approaches taken by such other agencies may well include the use of regulatory tools which could benefit NRC Safeguards enforcement. All of the procedures and mechanisms of other agencies will have their counterparts among those used in the civilian nuclear industry, but they may be wielded in ways which could shed new light on their potential in the NRC regulatory area.

It is to these other regulatory areas that we now turn.

D. RESPONSE TO REGULATION

Regulated industries respond to the requirements of regulation on two principal levels. The first is what they are required to do. The second is what they do of their own accord because they deem it in their best interests to support the same objectives which concern the regulators. Optimum results flow from the confluence of responses on these two levels. Substantial responses on the second level depend, however, on industry perception of the threat to be guarded against.

In the white-collar crime area, for example, regulated enterprises will respond far more vigorously to the dangers of employee embezzlement or low-level peculations than they will to requirements directed against high-level executive abuse. Thus a bank's auditors will closely monitor the flow of bank funds, but not necessarily check to determine whether bank officers have made loans to businesses in which they have an interest; criminal cases against bankers for making loans do not as a rule develop out of internal audits. Business steps which might violate laws against price-fixing or monopoly will receive internal scrutiny (or scrutiny by outside counsel) to determine whether the proposed actions are far enough on the dark side of the "grey" area to trigger government or private legal reactions or criminal action, rather than whether the steps are lawful per se.

There are many areas of activity in which businessmen do not perceive proscribed activities to be truly wrong, even though illegal --- such as cases involving anti-trust violations, misrepresentations or misleading material in advertising, marginal questions of customer safety when a new product is to be put on the market, and trading in securities on the basis of inside information. In some instances resistance to regulation is based upon the out-of-pocket costs of conducting business as required by law; in other instances resistance is based upon concern about not being able to make sales or special profits, or frustration of some other personal or corporate objective. In these instances the main burden of regulation generally falls on the government, since little voluntary support is to be anticipated.

In the civilian nuclear industry, it can be anticipated that Safeguards objectives, insofar as they relate to diversion or sabotage are totally in accord with licensee objectives, though there will be differences of opinion as to the level of perceived threats, and whether certain levels of threats are worth the dollar costs to counter them. Since common agreement on Safeguard threats, as between licensees and the NRC, is not consistently achieved in the non-white-collar crime area, it can be assumed that licensees will also resist incurring Safeguards costs in the white-collar area beyond their assessment of the likelihood of successful white-collar thefts and the expected direct and indirect dollar costs of such violations. If the NRC perceives this to be a Safeguards risk area, it will have to pay special attention to it.

Outside the nuclear regulatory area there may be these principal industry inputs to regulatory structures: (1) license conditions; (2) provision for maintenance of records subject to inspection; (3) reports and certifications to be made by the licensee; (4) audits by independent certified public accountants, and filings of reports approved by outside authority (independent counsel). These are discussed in turn, in conjunction with the nuclear regulatory area.

(1) License conditions. As noted above, there are rather fundamental differences between license conditions in the civilian nuclear area and other regulatory areas.[43] "Licenses" to banks, airlines, etc., are more likely to deal with such issues as situs of operations, qualifications of management, and operating capital requirements. There is little experience to be transferred in this area.

(2) Record keeping requirements. Regulatory requirements uniformly mandate maintenance of records which form a basis for inspection, for following a financial or other operational trail. The proper maintenance

---

[43]See p. V-2, supra.

of records is sometimes given a legal status separate and apart from questions of theft or diversion, i.e., it is a federal crime to deliberately make false entries in the books of a federally insured bank, regardless of whether money or property was actually taken. Violations in other regulatory schemes, for example laws dealing with banking and securities, often will provide for specific criminal penalties for violations in the particular regulatory area and do not rest on laws of general application dealing with criminal offenses against the Federal Government or in frustration of its policies.

(3) Reports and certifications. Periodic reports and certifications are commonly required by regulatory agencies. These reports and certifications are handled in two ways. Some are deemed important for operational reasons, and are very exhaustively reviewed. Others are relied on to surface indications of possible violations or regulatory problems. This latter purpose is a most important one in situations where many reports cannot be exhaustively reviewed, and is supported by the sanctions in 18. U.S.C. 1001 which provides that it is a felony to make a material false statement, or to conceal a fact which would be material to the making of an administrative decision or determination. The potential utility of this tool has been described as follows:

> . . . . If regulatory agencies or government departments have the power to make decisions and to ask questions in aid of their decision making functions (whether to buy, or to grant licenses or permits for specific activities), then criminal sanctions can be invoked if these answers be false. Put another way, public objectives may be advanced via white-collar criminal processes by asking questions which induce particular action or conduct, since favorable exercise of government discretion will depend on the answers . . .[44]

Section 1001 can be a potent tool when the reports and certifications are used to look for indicators of white-collar crime or related violations, and not merely to surface blatant wrongdoing. In the nuclear regulatory field, for example, the question whether any material records have been "corrected" may be a more potent tool than requiring an individual report on every document correction. An explanatory report could be technically accurate but somewhat misleading, while a general report that a correction was made is more likely (if there is a follow-up) to result in closer scrutiny of the transaction. If there is an investigation, the fact that no one had in fact looked at the deliberately misleading report would be no defense to a false statement charge; the crime is depriving the regulator or administrator of the option.

---

[44]See Edelhertz, op. cit., Note 2, p. 67.

(4) Independent reports. Regulated parties use the services of independent certified public accountants, independent legal counsel, and consultants to serve a variety of internal needs and external regulatory or other legal requirements. Publicly owned corporations must have certified financial statements to comply with S.E.C. and other reporting requirements; legal counsel sift data bearing upon company operations in connection with periodic reports filed in compliance with S.E.C. or other reporting requirements. The professionals who prepare such reports assume legal responsibilities, i.e., they may be liable to costly legal actions for negligence or may suffer crushing professional blows if debarred from practicing before or representing their clients in matters before a particular regulatory agency.

Such professional services are a valuable supplement to regulatory agency surveillance, since the work necessary to prepare these reports and opinions will often be far more searching than that which the regulatory agency can undertake.

In the civilian nuclear industry it would appear that independent auditors do make a contribution in the review of licensee record systems, but do not fully assume the level of responsibility for checking material inventories which they do in their work in other industrial and commercial areas. The reason given is that there are special factors involving security and expertise which make it more reasonable to permit them to rely on physical inventories taken by licensee personnel. It is not at all clear that these difficulties are so great as to preclude increased responsibility of independent auditors for verifying physical inventories.

Specific provision is made in NRC regulations for outside, independent critiques of licensee Safeguard procedures.[45] There appear to be no clear standards for activities of the review groups making these critiques. While their findings are open to NRC inspectors, they are addressed to the licensees and do not leave licensed premises. These Safeguards review groups clearly have substantial potential for addressing the subtleties of vulnerability to white-collar adversaries, but NRC should be a primary rather than indirect beneficiary of their services. The fact that these review groups are established pursuant to license conditions, and that their reports can only be reviewed on-site by NRC inspectors, leaves open the question whether they currently meet their full monitoring potential.

E. REGULATORY AGENCY CONTROLS

NRC Safeguards activities rest on these bases: (a) regulations, regulatory guides, instruction and informative memoranda to licensees as as a group, and individual license terms and conditions; (b) monitoring of records and reports reflecting nuclear material transactions and movements outside licensed facilities; (c) visits by inspectors to licensed

---

[45]See 10 C.F.R. 70.58(c)(2).

facilities to make assessments of how Safeguards operations are executed in practice; (d) post-audit reviews of paperwork generated in the course of nuclear industry transactions, at central locations, or during inspector site visits to nuclear facilities; (e) verification of nuclear transactions or movements by comparison of paperwork generated by all parties to a single transaction to determine whether they are consistent with one another; (f) follow-up requests for information and/or by investigation with respect to poor practices or procedures, or suspected violations; (g) invocation of remedies, administrative, civil, or by criminal reference; and (h) supportive research.

The framework for growth of the Safeguards response to white-collar crime and related abuses is clearly present. Two points must, however, be stressed. The first is that greater NRC orientation to this problem should be undertaken, so that white-collar crime issues are taken more into account at all the points referred to above, including systematic searches for applicable methods and approaches from other regulatory agencies. The second is that attention must be given to making Safeguards and non-Safeguards monitoring and inspection systems mutually supportive of one another. In the course of this relatively short survey, the impression was received that there is little coordination between these functions at any level --- though these separate organizational efforts are cited as a redundancy element contributing to the integrity of records and material inventories so vital to Safeguards efforts in the white-collar crime area.

F. EXTERNAL INPUTS

External inputs are those which stem from the public, media, licensee stockholders, other parts of the executive branch, state governments, and the U.S. Congress. As noted above,[46] most of these inputs (affirmative or negative, friendly or hostile) have been shaped by NRC, the civilian nuclear industry, and those who are in the industry or service it in some manner. Particularly in the white-collar area where vulnerabilities have not been exhaustively surveyed or assessed, there is need for reaching out for assistance in both framing issues for research and debate, and finding experience which can be adapted and transferred to cope with white-collar crime which does or could affect the achievement of Safeguards objectives.

---

[46] See p. I-5.

VI. THE CHALLENGE OF THE WHITE-COLLAR ADVERSARY TO REGULATION OF THE CIVILIAN NUCLEAR INDUSTRY

There seems little doubt that the scale of private commercial nuclear operations in the United States, and commercial relations between domestic licensees and foreign markets will greatly expand in the future --- which means that there will be many more transactions to be monitored. This, in turn, raises the possibility that Safeguards systems must be concerned about increasing numbers of white-collar adversaries, both here and abroad. In addition, illicit markets in nuclear materials, developing out of constraints on and other changes in the nature of the legitimate marketplace, may produce an expanding range of white-collar adversaries. The Nuclear Regulatory Commission will face these challenges with resources that are not likely to expand proportionately with the problems. It must therefore anticipate these problems, and design innovative and resourceful techniques to cope with them.

The white-collar adversary represents more a future than a present threat to Safeguards objectives, except in the narrow area of fraud relating to contract performance in connection with supply and construction of Safeguards protections at licensee sites.[47] Relatively, there is no reason to believe that the threat is less in the area of white-collar crime than in the area of overt crime by physical means; in fact, it may be a more serious threat because the adversary is less obvious and because commercial pressures for avoidance of national and international Safeguards controls may be expected to grow with the industry.

White-collar crime threats will be deterred by many Safeguards measures now in place. Many of the points made in this report are general to all Safeguards adversaries; the difference is that these points are of special importance in dealing with white-collar adversaries, or must be given different emphases in dealing with these adversaries. Material accounting requirements and detection devices, for example, make things difficult for the pilferer who tries to segregate stolen material within a facility and then carry it past a plant gate. However, these measures will more effectively hamper the adversary who seeks to avoid the system than the white-collar adversary who seeks to use the system against itself.

---

[47] While fraud committed in connection with licensee purchasing or construction activities will usually impact on the safety of licensee facilities rather than on Safeguard protections, there is no reason to believe that plant protective facilities will not sometimes be weakened by falsified indicia of compliance with procurement specifications. Coverups of construction flaws are just as possible with respect to perimeter barriers as they are in the case of reactor safety systems. This potential Safeguards problem is not addressed in this study. It may be conceptually difficult to distinguish it from other white-collar crime affecting the achievement of Safeguards objectives, but the authors of this report believe that it presents a quite distinct enforcement problem, one which would be better considered together with other (non-Safeguards) construction and procurement concerns.

In the presentation of the conceptual schema, Chapter IV above, the characteristics of the white-collar adversary and the character of his motives and acts were described as if they now existed and constituted a major threat to Safeguards systems. This was done for the purpose of providing information about the nature of the white-collar threat for use in shaping a response to this threat. However, no detailed assessment of the present nature or future potential of the white-collar nuclear threat has been made. Nevertheless, there are some observations relating to NRC Safeguards and the white-collar adversary threat which are appropriate here. The discussion following therefore focuses on two Safeguards issues that in our judgment are relevant to an assessment of NRC's preparedness to cope with present or future white-collar threats: (1) the concerns of Safeguards research and (2) the scope and sensitivity of current Safeguards systems.

A. THE CONCERNS OF SAFEGUARDS RESEARCH

Perhaps the most striking aspect of the considerable Safeguards research devoted to adversary threat potential is not the range of threats that have been considered, but the selective manner in which some, like the white-collar threat, have been given relatively little attention. Dangers from adversaries to whom much attention has been devoted, the terrorist, for example, are not necessarily greater in likelihood of occurrence or seriousness of consequence than are those associated with the white-collar adversary. To our knowledge, no armed adversary assault on a government or private nuclear facility to steal nuclear materials has occurred to date; neither can anyone state with complete confidence how likely and/or imminent such an assault may be. These two facts, however, have not prevented Safeguards researchers from in-depth analyses of the armed attack potential --- for the important reason that should such an event happen, the consequences could be extremely serious.

A similar argument can be made with regard to the white-collar adversary. To our knowledge, no white-collar adversary "assault" (of Safeguards' significance) has been made against any government or private nuclear facility; neither can anyone predict how likely and/or imminent such acts might be. However, unlike cases of armed or other "overt" assaults, no one can with any confidence state that a white-collar adversary action has not taken place to date. Further, while the immediate societal consequences of a diversion or theft by a white-collar adversary might not be as great as those presented by the successful terrorist or other armed assailant, the consequences could be serious indeed.

All this does not mean that the threat from the white-collar adversary should be moved to the front rank of Safeguards research concerns at the present time. There is need to know much more about this threat than we now know, and then there will still remain the question whether this threat calls for specific Safeguards system responses or can best be dealt with

by more generalized research and operational approaches. For example, in the case of computer fraud there is much concern about the dimensions of the problem outside the nuclear industry, especially since it appears that no major fraud of this kind has been detected by internal audits --- yet there has been no unique response, only intensified internal audit and verification of external transactions.

B. THE SCOPE AND SENSITIVITY OF CURRENT SAFEGUARDS SYSTEMS

Current Safeguards systems seem less attuned and sensitized to white-collar adversary acts than to other kinds of threats. As a result, several aspects which are predominant in these systems contain elements which do not appear fully capable of coping with the white-collar adversary.

First, a major part of the design of Safeguards systems rests upon the predetermination of those problems likely to be observed and the development of specific responsive measures to counter, sanction, and/or control, each. From the perspective of the white-collar adversary this approach falls short of the mark, not only because this adversary has not been a major part of the problem defined for the predetermined assessment, but also because he will be unlikely to generate observable actions to which responsive measures can relate. For example, the effort to predetermine the problems of the white-collar adversary as a basis for design of strategic and tactical Safeguards system responses should focus not only on the search for system weaknesses but also on the question of what records or activities would have to be altered or disguised in order to prevent discovery of a theft if one were to have successfully taken place.

The white-collar threat calls for Safeguards mechanisms that can anticipate the subtlety and disguised purpose characteristic of white-collar crimes. No matter how responsive Safeguards systems may be to observed situations, their ultimate capability to deal with the white-collar adversary whose acts will be concealed will depend on such anticipations which in turn must rest upon (1) a high level of awareness on the part of both NRC and licensee personnel of the tools and techniques of white-collar crime, and (2) a search for experience from outside the nuclear field which will help to anticipate and deal with this threat.

A second aspect of current Safeguards systems is that they place great reliance on redundancy in both procedure and record-keeping. While redundant checks are important control mechanisms, rigidity of redundancy when applied to both record-keeping and procedure can be more instructive to the white-collar adversary than a deterrent to him. The vulnerability of system routinization to the white-collar adversary was noted earlier (at pp. IV-10ff), but redundancy creates a more subtle vulnerability. This vulnerability stems from the lack of continuing NRC and licensee staff consciousness that develops once redundant mechanisms are in place. The more complex and sophisticated the design of redundant mechanisms, the more confident and less continuously vigilant the control system becomes which relies upon them. The idea that "nothing can happen here" is really the

first step toward assuring that "something" can indeed happen here. White-collar criminals have not found it too difficult to defraud experienced, successful businessmen notwithstanding intensive professional and legal scrutiny of fraudulent transactions. Sophisticated and confident control systems may be no less vulnerable.

The answer is not, however, to reduce reliance on the checks and balances provided by current Safeguards systems. Rather, the solution is more likely to be found in the development of a more strategic mix in the utilization of such tools. For example, redundant record-keeping mechanisms might be more usefully combined with procedural variability as a counter measure against possible white-collar adversaries. Here the variability would provide the system uncertainty necessary to more capably detect --- and hence to deter --- adversary acts. Such steps would, of course, have operational costs which would have to be carefully weighed against the benefits expected.

Another aspect of current Safeguards systems which should be considered in determining the appropriateness with which these systems deal with the white-collar adversary is their view of redundant mechanisms. Safeguards systems employ redundant measures within their own designs. In addition, they rely upon financial, quality control and external audit or measurement procedures to create further redundancy. Essentially, however, Safeguards remains a function and area of responsibility that is separate and apart from other facility and regulatory operations. This creates the danger that redundancy *potential* may be considered the equivalent of redundancy *in practice*.

NRC requirements call for quality control measurements and audits which serve both a quality control function and redundant check on production functions. Such requirements may theoretically serve as a check or verification for Safeguards purposes, but Safeguards authorities have no real way of knowing if a redundancy has been created which will be helpful even if they know that a quality control audit has taken place. The tendency to believe that procedures prescribed are procedures performed (and performed substantively) is inherent in complex organization structures. It is also a tendency on which the white-collar adversary may sometimes confidently rely. Consider the situation, for example, where a white-collar adversary (for any number of the motives described in Section IV) has diverted and hidden small amounts of nuclear material in a plant for later removal. If this has been done successfully (i.e., there is no basis for a suspicion that anything like this has thus far occurred), Safeguards systems may not have detected it and detection would rest on some other inspection function such as that of Health Physics which makes criticality checks.[48] In this instance, then, Health Physics could provide a control mechanism important to Safeguards.

---

[48]This assumes that such criticality checks provide general facility sweeps rather than spot checks in "normal" places, (i.e., where nuclear materials are expected to be found).

Safeguarding nuclear materials and facilities thus requires a breadth of scope that functional Safeguards separation may not provide. These are certainly not reasons, in and of themselves, for any joinder of functions, but rather an issue to be considered in Safeguards system design and implementation.

Strategies designed to combat the white-collar adversary should be sensitive to the elements of white-collar crime discussed in Section III, above. Safeguards systems which, for example, enhance the capacity to pierce an adversary's *disguise of purpose* or discourage his *reliance* on system weakness will heighten Safeguards systems' preventive potential. Steps which will make *victim voluntary action* less likely to be forthcoming, or make it more difficult to *conceal* or cover up implementing acts will have both preventive and detection value. For example, proactive steps to address the white-collar crime elements of *disguise* and *voluntary victim action* might be explored by inserting false documentation into a licensee paper flow to test ("black-hat") licensee defensive capabilities.[49]

W. Ross Ashby, in developing his theory of requisite variety and the regulator,[50] noted that the capacity of a regulatory mechanism to provide the level of system protection desired is a function of one major capacity. This capacity is the ability to meet variety introduced by disturbances (i.e., adversaries) to the system with equally varied detective and responsive mechanisms. Ashby's point here is that the capacity to regulate requires the capacity to anticipate, describe, and counter the varied challenges the regulator faces. He states it as a law: only variety can destroy variety; and only variety introduced by the Regulator can force down [reduce or counter] the variety introduced by system adversaries.[51]

From this perspective, regulatory vulnerability derives not from an inability to design control mechanisms or even to make rules carefully, but rather from an inability to correctly define the variety of challenges

---

[49]Such tests are currently being simulated with respect to physical assaults on nuclear plants because it would be highly dangerous to try a "live" test. No such dangers should inhibit a "live" test in the white-collar crime area, though some labor relations problems might be anticipated.

[50]W. R. Ashby, Introduction to Cybernetics, (New York: Wiley, 1956), see especially pp. 202-218.

[51]This is a paraphrase of Ashby's Law of Requisite Variety, which he states as follows: "only variety in R [the Regulator] can force down the variety due to D; only variety can destroy variety."

confronting the system to be protected. Failure to give proper recognition to the full range of adversaries confronting the nuclear industry produces the secondary effect of failure to create the regulatory variety necessary to counter such adversaries successfully.

END