2002

Organizational culture's contributions to security failures within the United States intelligence community

Troy Michael Mouton
Louisiana State University and Agricultural and Mechanical College

ORGANIZATIONAL CULTURE'S CONTRIBUTIONS TO SECURITY FAILURES WITHIN THE UNITED STATES INTELLIGENCE COMMUNITY

A Thesis

Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Master of Arts in Liberal Arts

in

The Interdepartmental Program
in Liberal Arts

by
Troy M. Mouton
B.A., University of Southwestern Louisiana, 1996
May 2002

DEDICATION

In memory of Lear Edward Olivier

Loving husband, father, neighbor

ACKNOWLEDGMENTS

I could not have completed this thesis without the guidance and expertise of the thesis director, Dr. Richard White. Dr. White's knowledge of the principles discussed in this thesis and his ability to encourage intellectual interrogatory are without parallel. For the instruction, counsel, and support Dr. White provided, I am in his debt.

The direction and contributions of Dr. Stephen Lucas and Dr. William Demastes were also instrumental to the completion of this project. Dr. Lucas's expertise in intelligence matters and Dr. Demastes's willingness to encourage a liberal arts education with interests in organizational culture have benefited the author immensely. Their experience, insight, and constructive criticism were invaluable. I am grateful for their patient consideration and willingness to share their extensive academic talents.

I will never be able to summon words that adequately express my love, gratitude, and respect for my wife, Glenis K. Mouton, who has supported me throughout my undergraduate as well as graduate education experiences. I simply owe everything that I am and will become to her.

TABLE OF CONTENTS

ABSTRACT

The institutions that comprise the United States intelligence community have organizational cultures that are unique from other government agencies. These cultures encourage the development and retention of traits that are necessary to mission accomplishment, yet these exclusivities also hamstring organizations and contribute to significant security failures. This thesis isolates elements of organizational culture specific to the United States intelligence community and explores the extent to which the culture is responsible for security and/or counterintelligence shortcomings.

For this thesis, the author selected three governmental organizations with intelligence collection and analysis functions: Office of Naval Intelligence (ONI), Central Intelligence Agency (CIA), and Federal Bureau of Investigation (FBI). The use of these agencies demonstrates that the intelligence community's military (ONI), intelligence (CIA), and law enforcement (FBI) components share common organizational traits.

The author subsequently identified a significant security failure case encountered by each agency and employed a case study approach to determine the extent to which organizational culture contributed to the security failures. Internal agency investigations and external assessments of espionage activities reveal that cultural factors impede the early detection of security compromises and thwart law enforcement efforts to investigate suspicious behavior.

Despite the deleterious effects of national security collapses, the intelligence community's personnel increasingly recognize the complicity of organizational culture in such security failures. The intelligence community increasingly analyzes the

negative aspects of its organizational traits, and there have been substantive strides within the intelligence establishment to minimize the security obstacles that organizational culture imposes on its constituent adherents.

The intelligence apparatus must maintain an organizational culture that distinguishes it from other government agencies. Unfortunately, the community's cultural characteristics also convey increased risks of security compromises. It is possible, however, for the United States intelligence community to maintain its unique organizational culture and minimize the possibility of operational or security failure.

CHAPTER ONE
INTRODUCTION

Organizations tasked with the collection and analysis of intelligence share cultural characteristics that distinguish them from most private sector groups and other governmental agencies that do not deal with intelligence matters regularly. Although certain cultural characteristics are as much a part of foreign (non-United States) intelligence agencies as they are central to the United States intelligence community, this thesis will concentrate on cultural concepts and the role they play in select United States intelligence agencies.

The organizational culture of the United States intelligence community allows the establishment to achieve operational objectives, but the same culture also contributes to security failures that continually plague the United States intelligence apparatus. Among the organizational culture characteristics that are specific to the intelligence community is the assumption that intelligence organizations will attract and employ individuals whose personalities, ideologies, and motivations are dissimilar from those of other government and private sector employees. Diverse value systems are also critical to the intelligence function, yet the necessity of divergent value systems poses significant risks to the security of intelligence functions. The intelligence community also stresses concepts such as limited information disclosure, extensive compartmentation policies, and routine counterintelligence protocols that border on paranoia. Other cultural attributes of the intelligence community include the degree of pre- and post-employment screening and security measures to which intelligence employees are subject. There are also numerous personal, public, and institutional

factors that contribute to and complicate the intelligence community's unique organizational culture.

It is extremely important for intelligence professionals to be aware of those cultural traits that are specific to the intelligence community because it is possible for individuals to act in accordance with those organizational culture principles while minimizing the possibility of security lapses due to exaggerations, abuses, and neglect of the intelligence culture's attributes. This awareness is exceptionally vital to intelligence managers and counterintelligence professionals who must proactively balance cultural necessities with the security weaknesses that organizational culture may exacerbate.

In its simplest form, organizational culture refers to the norms, values, and expectations that influence and govern the manner in which groups (or agencies) prioritize objectives and conduct their affairs. Culture also establishes acceptability parameters for behavior within a given body and details the consequences or results of nonconformance with underlying assumptions. Organizational culture is basically a theoretical explanation for the means by which an organization accomplishes its objectives (Schein 7). Contrary to common beliefs, intelligence refers to more than mere information. Information develops into intelligence when contextual analysis by persons or equipment capable of interpreting its relation to other information determines that it is of substantive value. Information becomes intelligence when the organizations that employ it in the decision-making process attach worth to it. Mark Lowenthal accurately notes that "[a]ll intelligence is information; not all information is intelligence" (Lowenthal 2).

In practically every organization, there exist belief systems, expectations, understandings, and concepts that affect the efficiency of the organization as well as the means by which groups and the individuals that comprise them attempt to accomplish given goals and priorities. Within organizations, there are also value systems at play that allow (and occasionally compel) employees to evaluate group dynamics and determine whether individual values and belief systems are compatible with or contrary to those exhibited by the organization or groups that comprise it. The combination of individual and community value systems with supervisory guidance/directive helps to define a system of norms and expectations specific to a given organization. The culture of the organization affects all aspects of its operation, including productivity, efficiency, and employee morale. Within those agencies that comprise the United States intelligence community (IC), however, organizational culture factors are more complex than in many organizations and impact far more than profitability.

The agencies, departments, and bureaus that comprise the United States intelligence community differ greatly from other governmental organizations due to their unique missions, methodologies, and organizational cultures. The organizational personalities that evolve in intelligence establishment entities are unavoidably necessary to the organizations' abilities to accomplish assigned objectives. However, the very characteristics that contribute to the intelligence community's unique organizational culture may also impede its ability to protect itself from security compromises and those who threaten operational security by disclosing classified information for ideological, monetary, or other reasons.

Given the nature of intelligence operations as well as the collection and analytical activities associated with such functions, it is not surprising that the risks affiliated with intelligence actions occasionally result in operational failures, security breaches, or counterintelligence shortcomings. Many intelligence functions face increased risks of operational compromise because of the intelligence community's reliance on sources and methodology that are susceptible to detection by its subjects' counterintelligence measures. In addition, many intelligence organizations encounter operational constraints that, although imposed by the agency sponsoring the collection and analytical activities, hamstring the organizations and ultimately prevent the intelligence agencies from detecting security breaches and identifying counterintelligence threats. In fact, the intelligence institution itself may be its own worst enemy in terms of security concerns by virtue of the operational attributes it embodies and the organizational culture it fosters among its members.

The purpose and mission of the United States intelligence community necessitate recruitment of employees whose belief and value systems vary widely. A diverse workforce combats homogenous assumptions and expectations that may result when groups lack diversity of values and beliefs. The extent to which employee value systems are consistent with or opposed to cultural expectations in intelligence organizations impacts mission accomplishment, employee morale, operational security, and counterintelligence efforts to detect security risks. The Pollard and Ames espionage cases confirm that poor employee morale may result in disenfranchisement with an agency's intelligence purpose and lead to operational security and counterintelligence shortcomings based on inaccurate predictions of employee behavior.

Furthermore, due to their responsibilities and the sometimes secretive manner in which they perform many assigned objectives, intelligence organizations have developed an organizational culture that requires and encourages secrecy, limited information sharing, and deep-seated suspicions of other agencies within the intelligence community. Naturally, intelligence professionals are even more suspicious of their peers who represent other states' intelligence and national security interests.

Military, intelligence, and law enforcement agencies of the United States that collect intelligence clandestinely and analyze classified as well as open-source information are the regular targets of other actors' intelligence establishments. Intelligence officers, analysts, and agents routinely engage in high-stakes cat-and-mouse analyses that draw on game theory principles. Intelligence professionals regularly analyze their collection actions and intelligence analyses in the context of "what-if" scenarios that allow them to consider as many possible consequences of their efforts and assessments. The extent to which their operations are successful depends on the agencies' insistence that employees adhere to cultural traits specific to the intelligence community. Naturally, operational success also hinges on opposing counterintelligence corps' detection techniques and the conduct of their own intelligence assets. However, even the most capable professionals and exemplary operations the United States has to offer are subject to increased failure risks due to internal security breaches and failed counterintelligence operations. The intelligence community's unique organizational culture contributes directly to its ability to sustain operational success and detect threats that could jeopardize intelligence operations.

One of the best-known icons of the United States intelligence community is the Central Intelligence Agency (CIA) and its headquarters facility located just outside Washington, D.C., in Langley, Virginia. The CIA's high profile may lead those who are unfamiliar with the intelligence community to assume that all intelligence operations involve the Agency's clandestine collection officers. In actuality, the intelligence community consists of at least thirteen agencies within the military, civilian intelligence, and law enforcement apparatuses.

Each of the Defense Department's military branches includes occupational specialties that are categorized broadly as "military intelligence." The United States Army, Air Force, Navy, and Marine Corps employ civilians and armed service members whose duties include intelligence, counterintelligence, and physical and technical security functions. The force strengths within each branch vary internally, but comparatively, the intelligence assets of the Army and Navy exceed the resources allocated to the Air Force and Marine Corps ("Agencies"). The armed forces intelligence components differ markedly from their civilian and law enforcement counterparts.

The military intelligence corps focuses, appropriately, on force protection issues, specifically the collection and analysis of intelligence that impacts or threatens the armed force operations of the United States and, increasingly, its allies. Military intelligence resources also respond to tasking from civilian intelligence agencies for specific collection requirements and perform extensive foreign language translation and interpretation duties of communications and signals intelligence collected by the National Security Agency. The branches also are responsible for other security

functions such as initial and periodic background investigations of service members whose positions necessitate access to classified information. To demonstrate that the cultural characteristics exhibited by civilian intelligence agencies are also commonplace in the military intelligence establishment, this study will include a review of the espionage activities of Jonathan Jay Pollard during his employment with the United States Office of Naval Intelligence (ONI) and the ONI's inability to identify the threat Pollard posed. The case study demonstrates that cultural traits expected of the CIA are inherent in other intelligence institutions as well, including the defense components.

As indicated by its title, the Central Intelligence Agency is by far the most renowned intelligence agency in the United States intelligence community; "intelligence" is in fact generally a synonym of the CIA acronym (Lowenthal 67). The National Security Act of 1947 created the CIA's predecessor, the Office of Strategic Services (NARA "Records"). The United States Congress enacted the 1947 legislation for two reasons. The public and its elected representatives sought to prevent another national security disaster such as the Pearl Harbor tragedy of December 7, 1941. According to many post-attack assessments, the United States could have prevented the Japanese attack on Hawaii if better information-sharing practices had occurred between military leaders and civilian intelligence professionals (Hitz 2). The National Security Act therefore sought to establish an information clearinghouse for national intelligence assembly and analysis with the expectation that improved communications and information sharing would diminish if not eliminate security failures due to inadequate communication channels (Hitz 2-3).

The OSS was the subject of severe criticism during its organizational infancy based on the agency's role in the Phoenix program during the Vietnam conflict. The Phoenix program was the OSS's controversial attempt to disrupt programmatically the rural apparatus that supported the Vietcong's need for soldiers and logistics by neutralizing Vietcong supporters and their bases in Vietnam and Cambodia (Karnow 616). The OSS eventually developed into the Central Intelligence Agency, and the current organizational structure divides the agency's functions among four directorates.

The Directorate of Administration and Training manages personnel matters to include employee hiring, training, transfers, payroll processing, and benefits administration. The Directorate of Science and Technology is responsible for technical analysis of photographic, satellite, and other imagery provided by agencies such as the National Reconnaissance Office (NRO). The Directorate of Operations (DO), or the clandestine service, is the arm of the CIA tasked with the overseas collection of political, military, economic, social, and other information relevant to the development and implementation of the United States's domestic and international policy agendas. The DO collects for analysis information that would not be available through overt channels. The Agency's Directorate of Intelligence (DI) performs all-source analysis of classified and unclassified information obtained by the DO and other intelligence agencies. The DI's analyses also influence domestic and foreign policy decisions made by members of the executive and legislative branches of government.

Each CIA directorate has its own agenda, and each division also has its own cultural traits. Throughout this thesis, reference to the CIA's organizational culture(s) will refer to the Directorate of Operations and Directorate of Intelligence because these

directorates best exemplify the cultural characteristics that contribute to security failures within the United States intelligence community. Analysis reveals organizational culture factors influence significantly the CIA's ability to detect and address security threats. The case study of the Aldrich Hazen Ames espionage affair demonstrates this fact dramatically. The review also highlights the stark divide between intelligence agencies and law enforcement agencies over the role of intelligence and the consequences of that philosophical difference on agencies' proactive security measures.

Unlike intelligence organizations, law enforcement agencies exist to investigate and enforce violations of various criminal statutes. To accomplish this mission, most law enforcement agencies receive investigative support from intelligence research specialists (or analysts) within intelligence divisions, departments, or groups. Whereas the CIA bears the responsibility for overseas collection requirements and may not collect information domestically, law enforcement agencies and the intelligence arms that support them must focus primarily on domestic concerns. Nonetheless, the investigative reality is that many law enforcement agencies, particularly the United States Customs Service (USCS), Drug Enforcement Administration (DEA), and Federal Bureau of Investigation (FBI), have the authority and need to pursue international leads in connection with complex criminal investigations. These agencies' exposure to international actors necessitates high levels of support from internal intelligence assets and formal liaisons with external resources to conduct thorough investigations. The case study of the espionage activities of FBI special agent Robert Philip Hanssen demonstrates that differences in intelligence and law enforcement ideology are surmountable. The study also indicates that when they are faced with security concerns,

law enforcement and intelligence agencies may be mutually dependent on each other to determine the source(s) of security failures and prevent unauthorized information disclosure or compromise.

The case studies of Pollard, Ames, and Hanssen capture dramatically the consequences of agencies' failures to detect or otherwise prevent security compromises that ended lives and jeopardized operations. The following chapters discuss the extent to which the intelligence community's organizational culture retains responsibility for those failures.

CHAPTER TWO
REVIEW OF LITERATURE

Organizational culture is more than a label or construct used to explain group behavior. In fact, culture is a phenomenon that occurs when a combination of characteristics assembles and creates a guidance system that influences both individual and group behaviors. This thesis will employ the description of organizational culture provided by Edgar H. Schein, who, in Organizational Culture and Leadership, defines culture as

> *a pattern of basic assumptions—invented, discovered, or developed by a given group as it learns to cope with its problem of external adaptation and internal integration—that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems*. (9)

Of particular relevance to the intelligence community is the reference in Schein's definition to external and internal difficulties. The intelligence culture, for example, requires internal integration of ideals, but procedural, ideological, and territorial rifts occur between intelligence community members when they must collaborate or apply a feasible internal mechanism externally.

Schein further describes various elements that explain culture in greater detail. He claims the levels of culture include basic underlying assumptions, values, and artifacts of the organization (13-14). Basic assumptions are the ideas and approaches that have been implemented so frequently as to become taken for granted. Basic assumptions represent the thought and action processes from which there is no variation or deviation since members of a given group or organization "would find behavior based on any other premise inconceivable" (18). These assumptions are similarly

described as "'theories-in-use'" or those nondebatable assumptions that guide behavior and instruct group members on how to think and feel about things (Schein 18).

The nondebatable assumptions of the intelligence culture include a workforce whose honesty and integrity are beyond reproach, employee screening (to include initial and periodic background investigations), compartmentation, need-to-know access principles, and guarded information sharing. A more detailed discussion of these assumptions will demonstrate that the basic underlying assumptions of the United States intelligence community and the role we expect it and, by extension, its participants or employees to play in the conduct of intelligence affairs represent the least significant threat to operational security.

Although some criticize what they consider a culture of secrecy, the public generally understands that the collection and analysis of intelligence demands that employees and institutions adhere to principles of secrecy and limited disclosure. Intelligence professionals, too, are generally cognizant that the manner in which the intelligence business gets done requires a mindset that appreciates the need for compartmentation and elaborate protocols for information access. Naturally, there are advocates who urge full disclosure of intelligence's operational funding, sources, and methodology, but such demands will not occur since they would undermine intelligence functions and could jeopardize the lives of individuals in the intelligence community. Difficulties arise, however, when the basic underlying assumptions of the intelligence community's culture become internalized excessively and restrict agencies' external adaptation abilities.

For example, intelligence organizations typically stress the need to protect the secrecy of operational details. Agencies safeguard such information in a number of ways, including pre- and post-employment briefings and physical as well as technical security measures. Occasionally, however, situations arise which expand the circle of those persons and entities with a need to know operational information. Unfortunately, intelligence agencies' prolonged practices of compartmentation and minimizing information circulation make expanding the need-to-know pool a difficult process. The task becomes increasingly complicated when the adaptation becomes externalized, or when one intelligence agency must (or at least should) share information with another organization that embodies the same culture. In such cases, even the basic underlying assumptions about the intelligence community, its purposes, and its protocols become clouded and contribute to its occasional inability to prevent or detect security failures.

The second level of culture addresses an organization's value systems. Unlike basic underlying assumptions, values are not universally autonomous responses or expectations. Values involve beliefs about what organizations should do rather than what they are expected to do based on cultural assumptions. Values stress the importance of prioritization and introduce the element of individualism to organizational culture. Although values may eventually become part of an organization's basic assumptions, whether this occurs depends on many factors, including leadership personalities, employee perceptions, and the success of previous value-driven approaches to problem solving. Among the intelligence community's most prominent value issues are degrees of information disclosure, importance of monetary gain, and significance of the intelligence mission.

When a value becomes an approach and the approach proves successful (or becomes socially validated), the value begins what Schein labels "cognitive transformation," a process in which values may become synonymous with or part of the basic assumptions of an organization (16). Clearly, not all values complete this transformation process successfully as values are intrinsically linked to individual beliefs and preferences that are not always malleable. Due to their individuality, values are exceptionally problematic to the intelligence community, and among the three levels of culture, they represent the most severe threat to security because of their unpredictable and influential nature. Whereas the first two levels of culture are fluid and intangible, the final cultural level consists of identifiable manifestations of an organization's underlying assumptions and value systems.

Schein labels the third cultural level as "artifacts," or the "constructed physical and social environment" of an organization (14). Artifacts include physical constructs, language patterns, and other outward expressions based on the other cultural elements. Among the artifacts specific to the United States intelligence community are physical and technical security measures, employee screening and disclosure requirements, and periodic reinvestigations of employees and their families. As the most overt and only visible element of the intelligence community's organizational culture, artifacts represent efficient tools that the intelligence establishment may use to address the threat posed by the other cultural elements, especially values. Essentially, the elements of culture as defined by Schein create an internalized system of checks and balances where divergent values, with the help of a culture's artifacts, prevent homogenization of assumptions that could create a bland organizational identity. As the following case

studies will demonstrate, however, individual values frequently usurp cultural artifacts and result in security failures.

Michael A. Turner echoes Schein and points out that organizational cultures are generally positive traits that occur when groups seek to define themselves and protect themselves from external environments or threats. Further cultural development typically ensues thereafter in an effort to maximize efficiency and organizational effectiveness, especially among subcultures (Turner 261-62). Turner's latter point is an especially accurate description of the DI : DO subculture dichotomy in the CIA. However, if the values of group members are contrary to the values of managerial personnel or the majority of the organization, the value difference may fail to optimize efficiency and result in what Schein considers a "socialization failure" that weakens a generally positive cultural apparatus (42). As demonstrated by the case studies that follow, if employee value systems "run counter to the pivotal assumptions of the total organization or the managerial coalition that is in power, the result can be active sabotage" (Schein 42). Undercutting these complications are individual motivations to pursue careers in intelligence and the dilemmas employees face after they enter the field.

Public service careers are not characterized by earnings potentials that are parallel to employee motivation and ability. Rather, civil service positions typically pay less than their private sector counterparts, have limited promotion potential, and compensate employees according to a regimented scale with little (if any) regard for individual creativity and productivity. In the 1960s, President Kennedy's call to "'ask what you can do for your country'" spurred commitments to national idealism and

swelled governmental ranks (qtd. in Hitz 15), but the dissolution of the Soviet Union and increased economic opportunities outside government service have lessened interest in public service careers. This description begs the question of what compels one to seek a career in public service, much less within a discipline with an organizational culture as complex as that of the intelligence community. The explanations are diverse and grounded in the theories of the humanist sociologist Abraham Maslow.

In 1943 Abraham Maslow published "A Theory of Human Motivation" and challenged long-standing beliefs that promoted the scientific management principles of Max Weber and Frederick Taylor. Whereas the Weberian approach to management emphasized concepts such as formal hierarchies and divisions of labor to increase and maintain productivity, Maslow suggested that humans seek to satisfy a hierarchy of needs that guide their behavior (Rosenbloom 144, 162). Satisfaction of these needs, Maslow argued, influenced employee behavior more than the rigid structure of authoritarianism touted by advocates of scientific management principles.

Maslow's hierarchy of needs included physiological, safety, social, self-esteem, and self-actualization needs (Rosenbloom 162). He argued that humans would first seek to satisfy physiological needs such as hunger and thirst before attempting to fulfill safety needs (such as shelter). Once workers satisfy these basic needs, they then seek social interaction that generally leads to increased self-esteem as a result of social identification with family and peer groups. It is only possible for one to achieve self-actualization (or true fulfillment) after having satisfied the basic predecessor needs.

Despite comparatively lower salaries than private sector employment, public service careers generally allow needs fulfillment along the Maslowian model. Career

public servants generally have more stable employment situations than non-governmental employees, and this stability tends to offer immediate satisfaction of physiological and safety needs. Civil servants may then address social and self-esteem needs since the organizations of which they are a part are generally less competitive and usually comprised of peers with similar interests. Satisfaction of the basic as well as social needs allows the public servant to achieve self-actualization through work-related responsibilities as well as functions not related to employment. In addition to these benefits, public service careers in the intelligence profession generally offer the added bonus of simultaneous needs fulfillment.

Intelligence professionals not only enjoy the same employment stability and benefits packages of other government employees, but they also tend to achieve self-actualization in concert with satisfaction of lower level needs. Intelligence careers tend to attract idealists who migrate towards careers that offer intrigue, prestige, a sense of accomplishment (or self-actualization), and peer recognition. A career in intelligence must provide such non-remunerative rewards since there are few occasions when employees may receive public praise for their efforts. In Organizational Psychology, Bernard M. Bass and Edward C. Ryterband discuss the importance of these and other employee motivation principles in their condensation of Maslow's needs theory into three broader periods of employee development whose characteristics are especially relevant to organizational culture principles. Their analysis is particularly important since the principles they address describe the reality of the intelligence culture as well as the obstacles such individual psychological factors represent to the intelligence community.

According to Bass and Ryterband, the key to employee motivation is "making the work itself more meaningful to the ego ideals of the employee" (41). The authors argue that other employment factors such as "supervision, coworkers, salary, working conditions, and company policies and practices…reduce dissatisfaction" but do not necessarily improve employee motivation (Bass and Ryterband 41). Employers that offer stimuli to encourage self-actualization enjoy a more productive workforce because "satisfaction accrues primarily from a sense of accomplishment in a job that has personal meaning" (Bass and Ryterband 42).

In Organizational Psychology, Schein echoes Bass and Ryterband's conclusions and predicts that managerial awareness of individual needs, combined with proactive supervisory controls on employee behavior, are essential to increased employee morale and organizational success (51). Schein indicates that according to the rational-economic assumptions managers make regarding employee motivation, employees will derive the greatest motivation from economic incentives and will behave in a manner consistent with income maximization (Organizational Psychology 52). The difficulty in applying this assumption to public servants is readily apparent since civil servants' wages are regulated and not specifically tied to individual productivity. Schein suggests managers adopt management approaches that identify and stress Amitai Etzioni's concept of calculative involvement to ensure control and minimize employee dissatisfaction (Organizational Psychology 54). Etzioni's concept essentially suggests that individual participation in an organization is based on "a calculation that participating in the organization serves some individual need" (Rosenbloom 158). However, as evidenced by the Hawthorne studies, there are numerous social factors that

also influence employee activity, and calculative involvement stresses employees' ideological needs rather than their social needs.

The Hawthorne studies demonstrated the importance of social factors and the extent to which employee production, satisfaction, loyalty, and predictability depend on the employee's social relationships within an organization (Rosenbloom 152). The studies revealed satisfaction of individuals' social needs necessitates a managerial approach that imposes authority without sacrificing ideals that are important to employees. The Hawthorne studies emphasized the importance of ensuring work assignments, peer interaction, economic incentives, and other reward systems address the higher level needs of the employee. Schein correctly argues that awareness of the rational-economic basis for action combined with a managerial strategy that addresses social needs allows employee self-actualization. This approach also encourages employee development and allows for unthreatening managerial oversight. Application of such a management strategy is likely to result in reduced levels of employee dissatisfaction that may lead to security failures based on a return to self-centered goals inherent in the rational-economic model.

In the intelligence community, potential employees are attracted to the unmeasurable benefits of the career, but the absence or weakening of subjective motivators may spell disastrous consequences for the employee who requires the psychological reinforcement not available otherwise. When the opportunity for self-actualization diminishes, the employee "encounters a work environment that gradually erodes the initial importance he had placed upon intrinsic task satisfactions and promotional rewards. Although the socioemotional rewards of his work context

remained relatively important, eventually work becomes far less meaningful for him" (Bass and Ryterband 61-62). Employees who experience this degree of dissatisfaction are prone to disassociate themselves from the organization and its mission and represent a significant threat to operational security. Aldrich Ames, for example, concluded "'the espionage business…was and is a self-serving sham, carried out by careerist bureaucrats who have managed to deceive several generations of American policy makers and the public about both the necessity and value of their work'" (qtd. in Corn 35). Employees who are most likely to experience this level of dissatisfaction include individuals whose motivations warrant the designations of "climbers" and "mixed motive employees" (Thomas 400).

Anthony Downs considers "climbers" those self-interested bureaucrats whose actions and behavior are motivated "almost entirely by goals that benefit themselves rather than their bureaus or society as a whole" (qtd. in Thomas 400). Among civil servants, this trait is most likely to manifest itself after a significant period of employment has lapsed. Within an intelligence organization, a climber "cannot exist for long…because the organization's overwhelming norm is loyalty to something other than the self" (Thomas 404). On the one hand, employees who exhibit extreme resentment towards and dissatisfaction with their organization are most likely to exhibit climber characteristics, and in most cases should attract the attention of an intelligence organization's artifacts (or security detection mechanisms).

Mixed-motive officials, on the other hand, tend to have more complicated identity issues and may prove more troublesome to identify. Downs holds that mixed motive employees "combine self-interest and altruistic loyalty to larger values" (qtd. in

Thomas 400). In the intelligence community, mixed motive officials "are far more common than purely self-interested individuals because most…careerists have some degree of altruism" (Thomas 406). Whereas these traits are desirable and perhaps even prerequisites for those pursuing public service careers, the characteristics may also create conflicts between the organization's values and those of the individual. Jonathan Pollard, for example, eventually concluded the United States's (and therefore the ONI's) value system was not commensurate with the values of his personal ideology. Because his motives were not those of the careerist and sought little self-serving purposes, his actions represented a greater threat to operational security because his espionage activities were less likely to attract the attention of supervisors and security authorities.

The personal motivation issues that complicate the intelligence community's organizational culture are highlighted further by various organizational factors that contribute to its unique culture. Weber postulated that secrecy was a necessary characteristic of any bureaucratic operation because it reinforced the hierarchy of authority that he believed was central to effective public administration (Rosenbloom 146). If any of Weber's scientific management descriptions are applicable to the intelligence community, the call for secrecy is it. Secrecy requirements are especially noticeable during the employee selection process, and the most common examples of the secrecy concept include personnel security principles such as the need-to-know principle, background investigation, and polygraph examinations (Wettering 270).

The need-to-know principle requires that "employees be given access only to those secrets that they need to know and no others" (Wettering 274). An extension of

this principle is compartmentation, or "restricting access to secret information to only those with a need to know" (Wettering 274). During the applicant screening process, it is not uncommon for intelligence organizations to advise prospective hires to limit the extent to which they disclose their career ambitions to anyone who does not need to know details of the position sought by the applicant. This recommendation serves two purposes. First, limiting the disclosure of information introduces the applicant to the industry standard of limiting information to only those persons with a legitimate need to know. Second, minimizing the disclosure of such seemingly trivial information may prevent security failures should the applicant actually become a member of the intelligence apparatus. Simply put, the risk of compromise increases with the rate of information disclosure.

Another truly unique characteristic of the intelligence community's organizational culture is the necessity of determining applicant suitability through the use of comprehensive background investigations. Periodic investigations of intelligence officers and analysts are also routine and generally occur in five-year intervals. As artifacts of the intelligence culture, such investigative measures, when used effectively, may provide valuable information on an individual's suitability for employment and susceptibility to the influence of other countries' intelligence services. Unfortunately, although such investigations are obviously beneficial security precautions, the "number of people to be screened is beyond the capabilities of the U.S. counterintelligence establishment" (Wettering 272). In addition to background investigation tools such as financial reporting (disclosures) and interviews of associates, intelligence organizations'

pre- and post-employment use of the polygraph examination is another cultural icon that is unique to the intelligence community.

The polygraph examination is an artifact of particular benefit to the intelligence community's counterintelligence corps. Counterintelligence, of course, refers to the proactive efforts that seek to deter information disclosure to unauthorized recipients, distort operational details through the use of misinformation, and identify internal threats to secure operations. Although the reliability of the polygraph examination is debatable, the tool serves three specific counterintelligence purposes:

> First, they intimidate would-be disclosers of secrets from doing so for fear of being caught. Second, when used on a routine basis they can reveal deceptions that can lead to confessions, or at least intensive scrutiny. Third, they can be used as a follow-up investigative tool should a person come under suspicion from other means. (Wettering 273)

The need-to-know principle, background investigations, and polygraph examinations are necessary security principles, but collectively they contribute to what many consider an undesirable culture of secrecy.

Former Senator Dennis DeConcini (D., Arizona) once chaired the Senate Select Committee on Intelligence and observed that the CIA, and by extension the intelligence community, have a "'culture of secrecy' that induces intelligence people [to] have a hard time being straightforward" (qtd. in Turner 260). Congressman Dan Glickman, past chairman of the House Permanent Select Committee on Intelligence, also noted that intelligence agencies tend to "deny that they are doing anything" (qtd. in Turner 260). Glickman also noted that in the intelligence community "[t]here is a cult of protectiveness, and it runs counter to any external review of their operations" (qtd. in Turner 260). The legislators' observations pinpoint one of the many difficulties that

plague the intelligence community's organizational culture. Intelligence agencies must treat employees differently than other bureaucratic institutions and conduct their affairs behind a veil of secrecy, yet in so doing they run the risk of excessive introversion and alienation from their peers, policy makers, the public, and the media. These intelligence community properties also have significant post-employment psychological ramifications for individuals who pursue careers in intelligence.

Earlier references alluded to promotional opportunities (or the lack thereof) within the intelligence community as factors that affected interest in intelligence careers. Upward mobility options also concern veteran careerists, yet the culture of the intelligence community historically has sent troubling signals about the bases for promotions. No governmental organization would admit that promotions are based solely on individual quotas or empirical data. After all, unlike private sector interests, government service stresses the delivery of services, which are generally not quantifiable, as opposed to the delivery of goods, which are easily recorded and analyzed.

In the intelligence community, however, and particularly in the CIA's Directorate of Operations, officers with the highest number of agent recruitments generally have received promotions (Riley 256). Critics allege that "numbers of recruitments are what matter…with quality playing second fiddle to quantity" (Riley 265). Furthermore, prior to the terrorist attacks against the United States on September 11, 2001, many intelligence professionals encountered hierarchy of needs conflicts due to a lack of mission clarity and purpose that prevent achievement of self-actualization. Rather than focused, goal-oriented directives, the intelligence complex has had "lots of

people doing many things on many fronts, rather than a focused few going against top priority targets…because there are no top priorities, just sundry demands" (Riley 258). The Ames study will demonstrate the accuracy of these arguments and illustrate the negative impact of such policies on individuals' assessments of their peers, supervisors, and the organization(s) they represent. The discussion will also address how political pressures affect employee perceptions of agency mission and the importance of the individual's contributions to it.

Intelligence agencies exist to assemble and collect information to create intelligence products that assist policy makers in the formulation and implementation of United States foreign and domestic policies. The intelligence community therefore has dual spheres of accountability. Organizations must respond to executive directives while complying with both executive mandates and congressional oversights. This accountability to two branches of government automatically politicizes organizations that should be immune from political pressures and contributes to the post-employment conflicts some intelligence professionals encounter. On this subject, John A. Gentry cites the comments of Jennifer Glaudemans, a former analyst in the CIA's Directorate of Intelligence. Glaudemans claims that "politicization is like fog" (qtd. in Gentry Ch. 6). She also states that "[t]hough you cannot hold it in your hands, or nail it to a wall, it does exist, it is real and it does affect people's behavior" (qtd. in Gentry Ch. 6) Nevertheless, executive and legislative requirements require mandatory specialization within and across agencies that contributes to individual and cultural conflicts which impact security failures.

Intelligence collection and analysis are separate functions that necessitate divisions of labor reminiscent of Taylorist scientific management principles. This functional division is especially noticeable between the CIA's Directorate of Operations and Directorate of Intelligence, where the basic intelligence culture is subdivided further between the directorates. There is a longstanding rivalry between the DI and DO regarding whether intelligence collection or analysis of the raw product is more important to policy considerations. The DO views its role as superior to the DI since the collectors assemble the crucial intelligence that would not otherwise be available to policy makers. The DI, in turn, routinely views its role as more important since its integration and analysis functions render the crude intelligence usable to policy makers.

Gentry notes that the culture in the CIA's DO "contains a streak of independence and contempt of accountability" (Gentry Ch. 3). He also contends the DO "jealously guards its information holdings, including those that could be of use to the analytic community" (Gentry Ch. 3) Gentry cites former Directors of Central Intelligence James Woolsey and John Deutch as acknowledging the importance of cultural change in the DO (Gentry Ch. 3). Once again, the information sharing component of the intelligence community's organizational culture reflects the difficulty that arises when organizations seek to balance need-to-know requirements interdepartmentally without jeopardizing the overall intelligence agency mission.

The information sharing variable and the following factors are among the most significant contributions to intelligence organizations' unique cultural traits. As mentioned previously, employee motivations to pursue careers in intelligence are diverse and complex. A cultural oddity of the intelligence community is the exhaustive

hiring process prospective applicants must complete in order to receive a formal offer of employment. Applicants must successfully complete various interviews, psychological assessments, and a battery of investigative reviews to determine suitability for employment. Employees must complete these processes mindful of the compensation disparities between government and the private sector. Hitz notes this problem and argues that to improve the intelligence community "a campaign should first be mounted to lure the best and the brightest men and women to intelligence work" (19). Hitz also suggests that "[t]hese top candidates must be paid a premium" (19). Additionally, employees generally must commit to mobility agreements that subject them to frequent travel and reassignment based on the best interests of the government. Although applicants receive notice of these conditions of employment prior to initiation of the hiring process, these procedures have few parallels within much less outside government and reinforce the distinct nature of their career choices. This knowledge may instill in the employee a sense of invincibility and egoism that complicate ideological constructs and may lead to disappointment, dissatisfaction, and disenfranchisement with the intelligence mission.

Earlier reference mentioned the direction and guidance that executive and legislative branches of government provide to the intelligence community. Whereas multiple spheres of accountability may create difficulties for intelligence managers, it is especially vital that intelligence organizations receive detailed direction to retain a sense of mission and purpose. Referring to the intelligence community, former DCI Richard Helms commented that "[t]here is no sense of mission" (qtd. in Turner 269). Bass and Ryterband suggest that "[w]hat holds us to the job, our satisfaction with it, is

determined by the extent the job is rewarding to us relative to how much better we might do elsewhere, what aspirations we have and what needs are fulfilled by our remaining on the job" (68). Riley suggests that the "intelligence requirements being handed down by policymakers today are many, while vision, direction, and leadership among those same policymakers is [sic] in short supply" (257). Without adequate direction, intelligence careerists are more likely to become dissatisfied with their employment, question the ideological importance of their functions, and seek self-actualization through alternative means. Some of these means represent significant security threats to intelligence operations.

Within the intelligence community, staff-level employees must believe that their assessments of peer behavior have significance and may contribute to supervisory decisions regarding corrective actions and promotion recommendations. If managerial personnel fail to consider peer reports and suggestions or act in a manner that suggests supervisors are accountable to a lesser standard than staff employees, they risk alienating their subordinates and may cause employees to question whether the position they sought on largely ideological grounds retains the primacy it once offered. Unfortunately, the intelligence community's organizational uniqueness only becomes more complicated when one considers the impact of ethnicity, counterintelligence, interagency territorial disputes, ideological problems, and legal matters on the organizations that comprise the intelligence establishment.

CHAPTER THREE
COMPLICATING FACTORS

The mission of the intelligence community necessitates the recruitment of personnel from different cultural heritages and academic disciplines. Intelligence agencies could not adequately perform what is expected of them if all employees conform to a single, universal mold. A workforce composed of talented professionals with various backgrounds, experiences, and educational disciplines ensures an array of values are represented since analysis of nation- or culture-specific intelligence requires diverse value systems. However, the intelligence community also depends on adherence to basic underlying assumptions that are not always consistent with diverse individual values. The conflict is obvious.

Rochelle Klein points out that "[i]t may be difficult or impossible to infuse common values and beliefs in such a diverse workforce" (Klein 323). She also indicates that "[e]lements of organizational culture may be incompatible with elements of ethnic cultures" (Klein 325). Klein contends that "[s]ome members of ethnic cultures may be unable or unwilling to become part of a particular organizational culture" (325). In Taylorist fashion, Klein also suggests that when this conflict occurs, "culture cannot be used as the form of communication and control" (335). She contends that a more "explicit, bureaucratic form of organization might then be more effective [since] bureaucracies may not require common values and basic assumptions in order to perform effectively" (335). The issue therefore becomes a question of whether intelligence organizations should abandon attempts to ensure cultural (ethnic) diversity because of the other cultural (value) risk it poses to security. For the reasons that

follow, the risks posed by different value systems do not warrant a homogenous intelligence apparatus.

An ethnically diverse intelligence corps is desirable because the persons with whom intelligence professionals must establish relations to collect and analyze human intelligence are themselves from diverse ethnic backgrounds. Ethnicity alone can be a useful intelligence tool; it is only logical for a recruited agent to feel more comfortable meeting with and providing information to an officer who shares the source's ethnicity. Furthermore, the common ethnical traits increase the believability of explanations for meetings between officer and agent. Wettering observes that "[m]ost of the more than 50 foreign intelligence services which operate in the United States…practice ethnic recruiting," and the United States intelligence community should continue to use this tool despite claims that it is discriminatory (275).

Maintenance of ethnic diversity is also desirable because it prevents the amalgamation of values that results in mirror-imaging. "Mirror-imaging" is the tendency "to view and interpret a foreign country's words and actions through one's own cultural optic, rather than from the perspective of the foreigners themselves" (Riley 263). Robert Callum accurately contends that mirror-imaging is "the fundamental weakness of the IC: with many intelligence professionals cut from the same cultural cloth, analysts share 'unacknowledged biases' that circumscribe both the definition of problems and the search for solutions" (Callum 26). "The solution," Callum suggests, "is to infuse the IC with a competitive heterogeneity of ideas, cultures, and mindsets by pursuing increased diversity and pluralism among analysts" (26). The increased diversity "will lead to improvements in analysis by lessening the impact of shared,

common biases" (Callum 27). Callum succinctly captures the importance of an ethnically diverse when he states that "[d]iversity in the IC is not a legal or ethical imperative, but rather an analytical one" (30). He correctly argues that "[t]o understand an increasingly complex world, an increasingly diverse work force is needed" (Callum 30). Despite the risks that divergent value systems may pose to security, "[c]ontinued reliance on a culturally homogenous pool of analysts will doom the United States to future 'intelligence failures' caused by the projection of 'our logic' onto the actions and tactics of antagonists" (Callum 30).

Finally, the intelligence community must seek ethnic diversity for ethical as well as operational reasons. Despite the complications that may arise from the presence of various value systems, intelligence organizations need an ethnically diverse work force to ensure that agencies do not encounter criticisms such as those encountered by the Office of Strategic Services and its incredibly homogenous intelligence cadre. Ethnic diversity should become yet another artifact of the intelligence culture that minimizes security threats rather than exacerbates them.

Yet another factor that complicates the organizational cultures of intelligence agencies is the need for and presence of counterintelligence assets. Counterintelligence (CI) efforts are generally offensive or defensive/technical measures that intelligence agencies employ to ensure the security of their operations. These measures contribute to more secure operations, but they also foster an atmosphere of paranoia among the intelligence community that exacerbates elements of distrust among intelligence professionals and limits information sharing and reporting of suspicious behavior. Offensive counterintelligence functions typically include recruitment, double agent

operations, and defensive measures including "surveillance, personnel and physical security, investigations, and police work" (Wettering 266). Physical security measures include the obvious safeguards of passwords, random searches, and password protocols. As mentioned previously, personnel security includes procedures such as background investigations and polygraph examinations, but a subsidiary component of personnel security includes programs that aim to detect employees with substance abuse problems, income and lifestyle disparities, and spousal issues that might affect employees' suitability for stewardship of classified information. The case studies that follow will demonstrate that across the intelligence organization spectrum, the community's disregard for these unique artifacts was largely responsible for the intelligence failures that occurred.

There are also administrative issues that complicate the intelligence community's organizational culture and the extent that culture affects security failures. As demonstrated by the Ames affair, many intelligence professionals question the efficacy of reporting problematic or suspicious employees whose actions constitute security threats. Supervisory responses to such complaints have not been productive. One reason for this lack of confidence in supervisory reactions stems from other cultural observations. The extant intelligence culture "not only protects its own, it punishes those who blow the whistle by objecting to lax discipline" (Turner 262). One intelligence official opined that "[f]ingering colleagues is considered unfair, leading to the failure…to punish individuals for past counterintelligence failures" (qtd. in Turner 262). An out-of-sight, out-of-mind mentality has been pervasive and resulted in unit reorganizations, transfers, and promotions of intelligence personnel whose actions are

not consistent with attributes that intelligence organizations value. Former CIA Inspector General Frederick Hitz noted that during his tenure at the agency "counterintelligence snafus didn't slow the advance of implicated officials but somehow served to advance them" (CIA OIG Abstract 17). Hitz noted that a "[s]crew up and move up" approach to addressing problem employee issues resulted in the promotion of personnel whose performance warranted discipline rather than praise (CIA OIG Abstract 17). Gentry echoes Hitz's observation and notes that one former analyst in the CIA's Office of Soviet Analysis observed how frequently supervisors received transfers and/or promotions:

> From April 1986 until August 1987, I had four different branch chiefs and from April 1985 until August 1987 I had four different division chiefs and I never changed jobs….When I worked on Soviet policy toward the United States from January 1988 until I left [CIA] in November 1989, I also had four different branch chiefs, two division chiefs and two group chiefs.

It is unlikely that such a promotion pace is attributable to exemplary performance. Rather, it is more likely that the high degree of turnovers in supervisory positions is at least partly attributable to transfers or promotions of supervisory employees whose performance was substandard.

Unfortunately, transfers and promotions of employees who pose risks to security sometimes occur despite coworkers' reporting of suspicious or inappropriate behavior. Management theorist Jay Forrester discusses the importance of employee reporting mechanisms and supervisory responses to such reports:

> If an organization is to deal with problems effectively, they have to be brought out into the open before they become too serious to manage. For this to happen, employees must know that managers will respond to the bad news itself, rather than shoot the messenger. They also have to know that, although it may not result in management action, all

> thoughtful dissent will receive a fair and honest hearing. This kind of open environment is particularly crucial if an organization is to surface potential ethical dilemmas, which there is great incentive to cover up. (qtd. in Pekel)

Gentry, however, notes that existing grievance systems in the intelligence community are inadequate counterintelligence tools. He cites a report issued by the CIA Office of Inspector General that charges "employees are loathe to use a grievance system to redress a wrong" (qtd. in Gentry Ch. 3). Employee distrust of supervisors and managerial mishandling of reported security violations leave employees few options other than submission of complaints to the various Inspectors General assigned to intelligence agencies. However, most employees are reluctant to utilize this resource as well.

The Office of Inspector General (OIG) is truly an ambitious concept. Supposedly, the OIG is an independent investigative arm that conducts civil and criminal investigations of a given agency and exercises additional oversight functions as well. The OIG is allegedly immune from the influence of agency chiefs and expected to enforce accountability standards without regard to political influences that might be brought to bear. Employees are oftentimes reluctant to report suspicious behavior to the OIG in recognition of the disastrous career consequences such actions may have on the individual reported should the allegations not be substantiated. Former Deputy Director for Intelligence Douglas MacEachen notes this hindrance and states that "the Inspector General will never come back and say you're absolved" (qtd. in Gentry Ch. 3). MacEachen also claims that the subject of an OIG inquiry "will never be definitely acquitted" (qtd. in Gentry Ch. 3). He contends OIG personnel "will say we found no evidence to substantiate it" but will never pronounce innocence (qtd. in Gentry Ch. 3).

Many employees therefore choose the lesser of two evils and allow managerial personnel to determine whether the information they provide on suspected vulnerabilities becomes the basis for more in-depth investigations.

Despite the inadequacy of these internal mechanisms to address security threats, and although law enforcement agencies have organizational cultures that in many ways are considerably similar to intelligence agencies, for the reasons that follow, intelligence professionals are loathe to request the assistance of criminal investigators and the intelligence assets of law enforcement. As do intelligence organizations, law enforcement agencies also have vested interests in establishing selective processes for hiring new personnel. The motivations of those who seek law enforcement careers are similarly unique to that profession as are the motivations specific to the intelligence community. Law enforcement personnel have understandable reasons for safeguarding operational information, and the agencies have probable cause to stress information disclosure guidelines given the nature of their functions. Law enforcement agencies and their staffs share significant cultural characteristics with their intelligence brethren, but the momentous differences in ideology between the organizations also contribute to significant security weaknesses. Observations of the historic relationship between the FBI and CIA will illustrate the difficulties mentioned.

Prior to the passage of National Security Act of 1947, the FBI had responsibility for the collection of all information related to espionage activities directed against the United States (Turner 263). In response to the attack on Pearl Harbor, however, Congress passed the 1947 Act to establish a national clearinghouse of intelligence to minimize the possibility of recurrent catastrophes. The CIA's predecessor, the Office of

Strategic Services (OSS), received responsibility for the collection of foreign intelligence and the conduct of covert operations outside the United States. Unlike cultural characteristics, the law enforcement : intelligence dichotomy and the restrictions that regulate the agencies are statutory.

Title 50 of the United States Code addresses war and national defense concerns. Section 403-3(d)(1) states that the Director of Central Intelligence (and by extension all other intelligence agencies) shall "collect intelligence through human sources and by other appropriate means, except that the Agency shall have no police, subpoena, or law enforcement powers or internal security functions." In addition, Executive Order 12333 further delineates what authority the intelligence apparatus enjoys to accomplish its directives and the point at which intelligence jurisdiction ends and law enforcement responsibility begins. Executive Order 12333 also states that one of the goals of the national intelligence effort is as follows:

> To the greatest extent possible consistent with applicable United States law and this Order, and with full consideration of the rights of United States persons, all agencies and departments should seek to ensure full and free exchange of information in order to derive maximum benefit from the United States intelligence effort.

Ironically, the cultural traits that the intelligence community shares with law enforcement agencies create rifts between the two complexes and handicap the information sharing principles that Executive Order 12333 suggests. The token information that the organizations do exchange is frequently insufficient, open-source material. The information's lack of intelligence value or delinquency of its delivery may result in preventable security failures. This unwillingness to share information

openly is attributable to the ideological differences between law enforcement and intelligence.

The differences between law enforcement and intelligence "are not only cultural…but legal, operational, and methodological" (Hulnick 275). One FBI counterintelligence officer observes that the FBI's approach differs markedly from that of the CIA. The official describes the intelligence approach as offensive and believes that law enforcement strategies tend to be defensive (Turner 265). These differences have "led to isolation…which engendered…the rise of separate procedures, separate points of view, and separate cultures" (Turner 265). Operationally, "intelligence officers want to exploit their sources and law enforcement personnel want to make convictions" (Hulnick 276). Former DCI Robert Gates also acknowledged these ideological differences and summarized them by declaring that law enforcement "wants to arrest and prosecute people and put them in jail, and the intelligence folks want to use information to get more information" (qtd. in Turner 265). For intelligence professionals, the "recruitment is not a 'one-time' deal" in that intelligence officers expect sources to be long-term producers of information that analysts can integrate to create predictors and assessments useful to policy makers (Hulnick 276). However, it is not unusual for law enforcement to recruit confidential informants for one specific operation. Despite their differing recruitment objectives, however, the law enforcement community is "just as eager to protect its sources, and is equally reluctant to divulge information outside the law enforcement community," much less trust disclosure of the information to intelligence agencies (Hulnick 276).

A recent report issued by the National Commission on Terrorism also echoed this problem. The Commission concluded that the "federal government is stymied by bureaucratic and cultural obstacles to the quick and broad collection of important intelligence" (qtd. in Kitfield "Covert" 2861). The Commission also determined that "law enforcement, defense, and intelligence agencies too often seem more interested in defending their turf than in coordinating their efforts and sharing sensitive intelligence" (qtd. in Kitfield "Covert" 2861). Ideological differences between law enforcement and intelligence are also compounded by legal concerns specific to the organizational functions of each group.

The law enforcement community's approach toward recruiting informants and collecting evidence stems from its mission of obtaining criminal convictions. Whereas intelligence organizations assemble and analyze investigative information that is not subject to rules of evidence, law enforcement seeks exculpatory information that can be introduced in legal proceedings to secure convictions (Hulnick 277). Convictions dictate criminal trials, and trials require the production of exculpatory information and evidentiary procedures that demand adherence to legal rules of discovery. For these reasons, law enforcement operations are held to legal and ethical standards not levied on intelligence agencies whose operations, most of which occur outside the United States, are not subject to legal restrictions imposed on law enforcement.

The 1948 trial of Judith Coplon further complicated (for the government) the dichotomy between evidentiary requirements and intelligence sources and methods. Coplon was convicted on charges of unauthorized disclosure of classified information after she was caught providing information to a romantic interest who was a KGB

operative. Coplon's legal counsel demanded and received the right to all FBI information related to the charges against the defendant. Although the FBI turned over most of the information subject to discovery, Coplon's conviction was overturned later partly because the United States refused to deliver information from the VENONA materials that identified Coplon's espionage activities (Wettering 290). VENONA is the code name that refers to the signals intelligence intercepts that allowed the United States to detect numerous cases of Soviet espionage conducted by Americans during the 1940s and 1950s (Lowenthal 102). The threat that secret information might be obtained by defense counsel is known as "greymail" and limits prosecutors' abilities to introduce classified information as evidence at trail for fear the information might compromise intelligence (or law enforcement) sources and methodology (Wettering 290).

Under discovery rules, evidence that may be introduced in criminal trials must be shared with the defendant's legal counsel, and because "this information must eventually be revealed to the defense in a trial, protection of sources and methods becomes impossible" (Hulnick 277). Compromise of sources and methods is anathema to both law enforcement and intelligence communities, but unlike intelligence organizations, law enforcement and prosecutors accept such disclosures as necessary to accomplishment of their missions.

In an attempt to address the problem posed by "greymail," Congress, in 1980, passed the Classified Information Procedures Act (CIPA). In compliance with discovery rules, the CIPA allows *ex parte* and *in camera* presentation of classified information to a judge so the court might determine, outside defense counsel's presence, (1) whether the disclosure of classified information is relevant to the legal proceedings

and (2) whether the release of that information would jeopardize current, former, or future intelligence or law enforcement operations (Wettering 290). Obviously, defense counsels must receive relevant information, but operational information that is not crucial to the prosecution or defense of the defendant is no longer subject to automatic defense scrutiny. The Department of Justice sought relief under the CIPA as recently as March 5, 2001, in its request to the court for a protective order to restrict the amount of classified information the prosecution had to release to Robert P. Hanssen's attorneys and further limit defense counsel's ability to share such information with the defendant (Frieden).

One of the unique characteristics of government is the difficulty of measuring the success of administration of public services. Empirical analysis of service delivery is generally not possible, so most surveys of government performance must measure subjective factors such as citizen satisfaction with a particular department or program. Like most other governmental agencies, the law enforcement and intelligence communities must demonstrate that their accomplishments warrant, at a minimum, continued funding levels, and, ideally, increased financial support. Agencies with intelligence functions therefore legitimize their budgets by measuring the number of sources recruited, analyses produced, and, to a lesser extent, catastrophes avoided. The budgetary logic simply assumes that *x* dollars will achieve *y* results. It also presumes that increased funding has a direct correlation with increased recruitments, analyses, and other intelligence products. This mentality is problematic in that it suggests quantity supersedes quality of information and may compel intelligence professionals to sacrifice ideals and values in favor of meeting recruitment and production quotas. As

was the case with Aldrich Ames, employees may compromise their own integrity and jeopardize operational security for the sake of career advancement influenced by inflated quota systems.

The organizational culture of the intelligence community is a complicated combination of assumptions, values, and expectations. Line-level intelligence employees and their supervisors have difficulty reconciling the cultural attributes with the demands of the profession. For example, the intelligence culture limits the extent to which intelligence professionals may discuss their employment with their partners. Additionally, intelligence employees typically may not publicize intelligence successes, but they must tolerate public and media criticism of alleged intelligence failures. The difficulty of this cultural balancing act is lost on the public, for its exposure to the intelligence community is limited, and its understanding of the intelligence community's unique organizational culture is practically nonexistent. Due in part to this lack of understanding, the public's perceptions of intelligence operations also impact (and complicate) the organizational culture of the intelligence community.

As early as 1830, Alexis de Tocqueville noted in Democracy in America that "democracies are not good at secrecy or perseverance in foreign affairs" (qtd. in Wettering 291). His nineteenth century analysis was on target then and remains accurate today. Americans by and large are intolerant of secretive governmental operations. Consider, for example, the public reaction to the Watergate episode of the 1970s. Public outcries for complete disclosure of operational funding, sources, and methodology are increasingly common. For operational reasons, full disclosure is obviously not possible, but part of the problem that nags the intelligence community is

its inability to broadcast the positive results of its efforts whereas the media readily reports on alleged intelligence failures and abuses.

Events such as the Iran-Contra affair of the 1980s and the CIA's recruitment of sources of information with alleged histories of human rights violations cause the public to question the ethical standards of intelligence. Such criticisms have become so influential that in 1995 DCI George Tenet issued what became known as the "scrub order," a directive restricting CIA officers' abilities to recruit agents with unsavory or questionable backgrounds ("Regulations"). Following the terrorist attacks of September 11, 2001, the CIA clarified the directive and asserted that "those guidelines have been changed to allow field officers greater latitude in making such decisions" (CIA "Terrorism"). Nonetheless, the issuance of the "scrub order" reflects Americans' inherent distrust of secrets and, to an even greater degree, informers.

When Linda Tripp produced audiocassette recordings of her conversations with Monica Lewinsky in which the former White House intern acknowledged salacious details of her relationship with former President Clinton, the public perceived Tripp as a disloyal tipster with selfish interests. In the public's eye, Tripp was an untrustworthy tattler who violated the sanctity of her relationship with Lewinsky (Wettering 291). Tripp's revelations labeled her an informer, and the United States public expressed its disrespect for her actions and motives. Clearly, intelligence organizations are not informers because the data collected and analyzed by the intelligence community does not serve the interests of individual agencies. The intelligence mission serves the interests of the United States's national security, but in order to assemble such intelligence, agencies must associate with persons and groups whose motives and means

are suspect. It is therefore only natural for the public to infer that intelligence professionals' mores are suspect also since members of the intelligence community sometimes must operate at the same level as the informants who provide intelligence. This connection simply reinforces the public's specific distrust of intelligence and general suspicions of government.

Historically, Americans have been apprehensive of a strong central government. The Articles of Confederation were intentionally weak because of this fear, and it was only after addition of the Bill of Rights that some states ratified the United States Constitution (Wettering 291). By necessity, intelligence organizations conduct most of their affairs in secret, and many assume secrecy translates to centralized, unchecked authority with little respect for individual rights and liberties. Civil libertarians routinely decry what they consider the intelligence community's culture of secrecy and argue that agencies' claims of the necessity for secrecy are merely obfuscations for the continued existence of a culture that ensures centrality of authority.

One of the most vocal advocates of openness in government is former United States Senator Daniel Patrick Moynihan. Moynihan's chief gravamen is that with the demise of a bipolar international system, there is no longer a need for the culture of secrecy that characterized the Cold War. He contends that a "culture of secrecy need not be the norm in the American government regarding national security" (Moynihan 55). Moynihan believes that "[t]o achieve greater efficiency, laws must be created to restrain the present culture of secrecy and promote a competing culture of openness" (55).

One of the armaments in Moynihan's arsenal of criticism is the incredible number of documents classified at the Confidential, Secret, and Top Secret level. Of particular concern to him is the government's unwillingness to declassify relics of bygone eras. Moynihan suggests that "organizations within a culture of secrecy will opt for classifying as much as possible, and for as long as possible" for both budgetary and authoritarian concerns (69). Just as lawmakers and senior government officials rely on recruitment figures and analyses as indicators for fiscal decisions, those in positions of authority also gauge agencies' need for funding in part on the number of classified documents an organization generates. Moynihan points to former President Clinton's Executive Order 12958 which, in 1995, resulted in over 374,244 documents receiving derivative designation as Top Secret for the information they contained. Moynihan's concern is legitimate, since excessive classification can impact negatively the agencies where organizational culture ingrained the initial determination that such classifications are necessary. Former Senator Moynihan suggests that the "system can become so constrictive that information is effectively withheld from those who need it" (64) Unfortunately, a cultural trait that allows the intelligence community to complete its objectives admirably under most circumstances may, in extreme circumstances, compete with itself and hinder the establishment's fulfillment of policy makers' and the public's expectations.

Given the problems associated with such information withholding, one might wonder whether agencies value budgetary allotments more than mission success. It would be unfair to make such an accusation since that stance applies a blanket distrust of intelligence professionals. Nonetheless, in fairness, it is evident that agency pride

and perceptions of strength and seniority are also complicit in interagency withholdings of intelligence. "Power in a culture of secrecy frequently derives from withholding secrets," Moynihan observes, and he points to the FBI's unwillingness to share with the CIA decoded VENONA messages until four years after the FBI received the information from the military intelligence assets of the United States Army (70). Despite the historical precedents in favor of increased information sharing and a revision of the culture of secrecy, Moynihan realistically points out that a "culture of openness will never develop within government until the present culture of secrecy is restrained by statute" (65). Such legislation, however, is far from imminent.

The preceding discussion has identified numerous cultural traits that are unique to organizations directly engaged in the collection and analysis of intelligence as well as those law enforcement agencies whose missions require adoption of specific cultural attributes. The cultural characteristics of the intelligence community include elements of secrecy, distrust and suspicion of peers and outsiders, severe compartmentation of information, and limited information sharing among community members. Other characteristics include employee motivation problems, compensation inequities, and conflicts that arise between ethnic and cultural diversity. Academicians and social scientists have recognized the unique nature of these traits, and organizational theory scholars as well as intelligence veterans have recognized that intelligence organizations must apply or exhibit these cultural traits in order to produce the product on which policy makers depend to make informed national security decisions.

Kent Pekel points to Paine's analysis and confirms that unethical behavior "*involves tacit, if not explicit, cooperation of others and reflects the values, attitudes,*

beliefs, language, and behavioral patterns that define an organization's operating culture" (qtd. in Pekel). Unfortunately, the organizational characteristics of the intelligence community compel it to be culturally insular and further distance the establishment from those segments of government and society that need not observe these cultural peculiarities (Corn 34). This separation contributes to assumptions about and misunderstandings of the intelligence community that exacerbate the perception of intelligence agencies as secretive, authoritarian entities that threaten civil liberties.

Applying Schein's organizational construct, the basic underlying assumptions, values, and artifacts of the intelligence community are responsible for significant security and counterintelligence failures. Review of the espionage activities of Jonathan Pollard, Aldrich Ames, and Robert Hanssen, and the cultural environment that allowed such behavior demonstrates that although their disclosures were unquestionably devastating to the intelligence community, there are valuable lessons to be learned from their behaviors and the organizational responses to those actions. It is probable that intelligence, counterintelligence, and security professionals will not detect all security compromises, but awareness of the cultural contributions to certain landmark failures may prevent future security and counterintelligence disasters.

CHAPTER FOUR
POLLARD CASE STUDY

On November 21, 1985, agents of the Federal Bureau of Investigation watched in anticipation and surprise as the green Ford Mustang they had surveilled throughout the morning entered the driveway of the Israeli embassy in Washington, D.C. The driver and owner of the vehicle was Jonathan Jay Pollard, an intelligence research specialist who worked for the Office of Naval Intelligence. Also present in the vehicle was Pollard's wife, Anne Henderson Pollard. The Pollards were the subject of FBI surveillance because just days earlier, the FBI and Naval Investigative Service had begun questioning Pollard about his unauthorized removal, possession, and distribution of classified national security information. Although Pollard had acknowledged during earlier interviews that he had inappropriately handled classified documents, agents did not arrest Pollard immediately since he appeared to be cooperating with their investigation and claimed to have additional information of relevance to criminal investigators and counterintelligence staff assigned to the investigation. Nonetheless, investigators were rightly suspect of the information Pollard had already provided, and the agents were concerned that if given the opportunity, Pollard would attempt to leave the United States. Agents were also hopeful that Pollard might lead the investigators to his handlers or foreign government officials on whose behalf Pollard had allegedly committed espionage. Their suspicions proved true, for out of fear, desperation, and a hope for a miracle, Pollard sought refuge and protection at the embassy of Israel, one of the United States's most loyal allies and the country on whose behalf Pollard had committed espionage.

Most states subscribe to an international legal standard establishing an embassy and the property on which it is located as the domain of the sovereign nation it represents. The Israeli embassy, for example, although physically situated in northwest Washington, D.C., is considered to be an extension of the Israeli State. Therefore, when Jonathan and Anne Pollard entered the Israeli embassy grounds, the agents surveilling the Pollards did not enter the Israeli premises because the embassy technically was considered outside the United States, and law enforcement agents had no authority to pursue their suspects. However, much to the Pollards' astonishment, shortly after their arrival at what they considered a safe haven from United States law enforcement, Israeli embassy officials demanded the Pollards leave the embassy. The government of Israel denied the Pollards the safe escape they had been promised, and with nowhere else to go, the Pollards departed the embassy grounds and were placed under immediate arrest by the FBI. As the FBI had hoped, Pollard had led agents to the front door of the state to which Pollard had disclosed significant amounts of classified national security information. Expecting a heroic reception from those whom he considered his fellow countrymen, Pollard received only a thankless dismissal.

Later that very Thursday, Jonathan Jay Pollard appeared before the Honorable Patrick Attridge, a United States Magistrate for the District of Columbia. Pollard learned that he was charged with violating Title XVIII, Section 794 (a) of the United States Code, alleging that Pollard, "during November of 1985…with intent and reason to believe that it was used to the advantage of a foreign nation, did communicate and deliver to a foreign government directly or indirectly documents, writings, and information to the national defense" (qtd. in Blitzer 181). If found guilty of this charge,

Pollard faced a maximum penalty of death, or imprisonment for any term, up to life. At the arraignment, Attridge also advised Pollard that he also was charged with violating Title XVIII, Section 793 (e) of the United States Code, "which makes it unlawful to possess any documents and writings relating to the national defense and willfully retain the same and fail to deliver them to the officer or employee of the United States entitled to receive them" (qtd. in Blitzer 181). The maximum penalty for conviction on this count was a fine of up to $10,000, up to ten years of imprisonment, or both.

Jonathan Jay Pollard was the first of two Pollards to appear before Magistrate Attridge for arraignment on criminal charges. On Monday, November 25, 1985, Anne Henderson Pollard also appeared and learned that she, too, was charged with violating Section 793 (e) of Title XVIII, United States Code, or "unauthorized possession and transmission of classified documents" (qtd. in Blitzer 187). Anne Pollard also faced penalties of up to ten years imprisonment or a fine of up to $10,000, or both, if convicted of this crime.

On June 4, 1986, Jonathan and Anne Pollard returned to the United States District Court in Washington, D.C. Jonathan Pollard advised Judge Aubrey Robinson, III, of his intent to plead guilty to conspiracy to commit espionage, or Title XVIII, United States Code, Section 794 (c). Anne Pollard similarly acknowledged her intent to plead guilty to one count of conspiracy to receive embezzled government property, in violation of Title XVIII, United States Code, Section 371. Anne Pollard also agreed to plead guilty to Sections 793 (e) and 3 of Title XVIII, which is accessory after the fact to possession of national defense documents (Blitzer 244).

The Pollards—indeed, most who followed the investigation—expected Anne Pollard to receive a suspended sentence based on her poor medical condition and plea agreement with prosecutors. Most watchers also expected Jonathan Pollard would receive a sentence of imprisonment of up to twenty-five years, a significant but reduced sentence based on his guilty plea and promise to cooperate fully with investigators. Government prosecutors had in fact agreed to recommend only a substantial sentence for Pollard instead of seeking the maximum penalty. Neither the Pollards nor courtroom observers expected the sentences Judge Robinson rendered. After having heard arguments by defense counsel and prosecutors for and against Jonathan and Anne Henderson Pollard, Judge Robinson pronounced

> With respect to the defendant Jonathan Pollard, who is being sentenced for violation of Title XVIII, United States Code, Section 794 (c), I commit the defendant to the custody of the Attorney General or his authorized representative for his life. With respect to the defendant, Anne Henderson Pollard, I commit the defendant Anne Henderson Pollard to the custody of the Attorney General or his authorized representative on the first count of the information to a period of five years. (qtd. in Blitzer 270–271)

At present, Jonathan Jay Pollard has served approximately 16 years of his life sentence. Anne Pollard has served her sentence and is no longer in prison. Jonathan Jay Pollard, however, remains incarcerated at the Federal Correctional Institution in Butner, North Carolina.

The basis for Jonathan Pollard's arrest for and subsequent admission to espionage charges began on May 29, 1984. On that date at the Washington Hilton Hotel in Washington, D.C., Pollard met with an Israeli representative and matter-of-factly advised his contact that "he wanted to provide classified documents and information," and he "described the position which he held and the nature of the

classified intelligence information and documents he could provide" (Blitzer 75). Over the next 20 months, Pollard would provide Israel with significant amounts of classified United States documents. Subsequent investigations and Pollard's confessions would reveal that Pollard "sold to Israel a volume of classified information ten feet by six feet by six feet" (Blitzer 259). Although he ultimately received compensation in exchange for his espionage activities, Pollard's initial motivation to provide Israel with classified information was not financial. His primary motive was ideological, and the factors that contributed to the value system that shaped Pollard's ideology represent one of the many challenges and difficulties of the intelligence community's organizational culture. Other organizational culture principles that contributed to the security failure represented by Pollard's espionage include physical and personnel security practices, information sharing principles, peer reporting norms, and spousal support for illegal activities.

Earlier discussions of employee motivations revealed that the intelligence community's objectives demand a diverse workforce for its information collection benefits and prevention of mirror-imaging tendencies. The intelligence establishment must therefore contend with employees whose value systems are far from uniform, and whose motivations for seeking careers in the intelligence field are equally diverse. Nonetheless, ethnic diversity is crucial to the United States establishment since such diversity prevents mirror-imaging tendencies and ensures a variety of viewpoints on intelligence matters. Among Schein's descriptions of the levels of culture, this author argued that cultural values are the greatest threat to the security of the intelligence establishment. In Pollard's case, this intelligence research specialist most accurately

fits the mold of Anthony Downs's mixed motive classification, and the inherent conflicts of such a personality run counter to the efficacy of intelligence organizations (Thomas 404).

Jonathan Pollard grew up in an academic environment. His father, Dr. Morris Pollard, was a respected microbiologist who served on the faculties of institutions such as the University of Notre Dame and Cambridge University. Dr. Pollard's career entailed periods abroad for the family and ensured Jonathan Pollard's exposure to elitism if not idealism through his familial engagement with scholars and academicians. The Pollard family also instilled in Jonathan Pollard the importance of his Jewish heritage, but whereas his parents were extremely pro-American, Jonathan Pollard's devotion was to Israel first and foremost. "For as long as I can remember," Pollard stated in an interview, "Israel has figured prominently in my life as an object of religious commitment as well as a source of personal strength" (qtd. in Blitzer 19). Pollard believed it was possible to rationalize illegal behavior through religious and nationalist justification so long as the rationalized behavior served a greater good than the wrong represented:

> I was brought up with the notion that this kind of service was not breaking the law but was the discharge, as I say, of a racial obligation. Certainly, it was made easier by the fact that as far as I was concerned…there was no difference between being a good American and a good Zionist. (qtd. in Blitzer 20)

Events in Israel only reinforced the ideologies to which Pollard had been exposed as a minor.

The 1967 Six-Day War greatly influenced Pollard's convictions about his duties to Israel. "That was the turning point for me," Pollard claimed (qtd. in Blitzer 25). His

concern over the possible destruction of Israel was complemented by a trip to the concentration camp at Dachau in 1968, which, he claimed, "gave palpable expression to the teachings of what could happen when Jews take their existence for granted," whereupon he came to believe that "every Jew had a responsibility, an obligation" to ensure that a catastrophe such as the Holocaust does not happen again (qtd. in Blitzer 27-28). These events collectively established a mixed-motive construct for Pollard, and his educational pursuits only reinforced what he considered dual loyalties to the United States and Israel.

After initially pursuing pre-medicine training at Stanford University, Pollard changed his major to political science. One of Pollard's former roommates recalled Pollard's interests included military history and intelligence operations, and he described Pollard as "definitely pro-Israel" (qtd. in Blitzer 35). Other collegiate associates recalled Pollard claimed to have worked for the Mossad, Israel's clandestine intelligence service, and even Pollard's father noted his son's fascination with intelligence. Pollard's father observed that Jonathan Pollard was "filled with romanticism" about a career in intelligence (qtd. in Blitzer 39). Pollard's commitment to a career in intelligence merged with his devout ideology in 1973 during the Yom Kippur War. It was during this event that Pollard "decided the intelligence field would provide…a skill which would be well received in Israel" (qtd. in Blitzer 40). Pollard's commitment to an intelligence profession, however, was blighted by his allegiance to Israel. Although Pollard was infatuated with pursuing an intelligence career, his allegiance to Israel overshadowed his loyalty to his chosen profession. Pollard believed that "[p]ersonal involvement was…the mark of a responsible individual" (qtd. in Blitzer

43). Blitzer observes that intelligence operations and the organizations that conducted them "simply could not satisfy that need" Pollard felt to make proactive contributions to a cause he considered more important than his professional obligations (Blitzer 43).

After graduation from Stanford, Pollard briefly pursued legal studies at the University of Notre Dame and graduate work at the Fletcher School of Law and Diplomacy at Tufts University. After his first year at Fletcher, Pollard participated in an internship at the Naval War College in Newport, Rhode Island. Pollard personally observed that "[t]he psychological hallmarks of divided loyalties were certainly there for all to see: the uneasy conscience, the sense of personal failure" (qtd. in Blitzer 47). Pollard notes that he was "becoming a weak man with good intentions and doomed by pride" (qtd. in Blitzer 47). Pollard, however, again rationalized his motivations. He believed that his commitment to Israel was not inconsistent with the interests of the United States. "They are not incompatible goals as far as I am concerned," Pollard claimed (qtd. in Blitzer 48). Having reconciled these incongruities, Pollard sought employment with the CIA but did not secure a position because of his drug use during college. The CIA's rejection of Pollard marked the beginning of his disenfranchisement with the intelligence apparatus, and his future employment with Naval Intelligence would only supplement his dissatisfaction with his chosen profession.

Pollard began his intelligence career as an intelligence research specialist with the United States Navy in 1979. Pollard immediately encountered what this author described as a homogenous intelligence structure that necessitated ethnic diversity among intelligence professionals. "I was totally unprepared for the level and extent of the anti-Semitism that was tolerated within the organization," Pollard later noted (qtd. in

Blitzer 52). His encounter with this cultural manifestation only reinforced his devotion to Israel and contributed to his voluntary disclosure of national security secrets. Pollard's experiences in Naval Intelligence only exaggerated his unhappiness. Anne Henderson urged her husband to leave the intelligence field, but Pollard remained. Pollard's continued involvement in intelligence allowed him to witness the United States's guarded information-sharing practices, and "he concluded that the United States was not providing Israel with enough classified information to enable it to strengthen its own military capability" (Blitzer 60).

The United States's reluctance to authorize complete disclosure of intelligence that might benefit Israel represents a hallmark underlying assumption of the intelligence community, the need-to-know principle. Pollard stated that he "concluded that those restrictions were inappropriate for Israel," and after the 1983 bombing of the United States Marine barracks in Beirut, he determined to "do something that would guarantee Israel's security" (Blitzer 63). Pollard later commented that he realized the illegality of his actions but allegedly determined "that the ends justified the means'" (Blitzer 63). Pollard's election to provide classified information to Israel without authorization based on individual versus organizational values represents one contribution of organizational culture to security failures. Another contributory factor, which is oftentimes an offshoot of motivation and value issues, is the influence of monetary gain on intelligence professionals.

Prior to providing information to the Israelis, Pollard voluntarily disclosed classified information to investment associates who, along with their clients, might benefit economically from the intelligence Pollard shared. According to Blitzer,

"Pollard told U.S. investigators that although he was not paid for the information, he hoped to be rewarded ultimately through business opportunities that these individuals could arrange for him when he left Naval Intelligence" (70). Pollard's admission that he sought financial gain from these disclosures is at odds with his later claims that he expected no remuneration from Israel for turning over classified documents. Despite his willingness to provide Israel free access to classified information initially, Pollard claims Israel forced him to accept compensation for his actions. Pollard stated that his handlers "would want him to like the extra cash, trips and presents" (Blitzer 79). Blitzer notes that the Israelis also wished for Pollard "to get used to a more comfortable lifestyle" (79). One might argue that, comparatively, intelligence careers do not offer lucrative compensation structures so that only prospective employees who share the basic underlying assumptions of the culture will pursue a career in the intelligence field. The rationale for such logic of course is that employees who share said assumptions pose a lesser risk of compromising security than those employees who do not accept the cultural assumptions of intelligence. Ironically, the lack of pay parity is actually a recurrent motivating factor in many espionage cases, including Pollard's.

Hired in 1979 as an intelligence research specialist, Pollard was, by 1985, quite accustomed to the improved lifestyle his espionage permitted. He received $2,500 monthly from Israel for his service (Blitzer 96). Apart from Pollard's ideological motives, the financial incentive alone was a threat to the public service motives that most government servants embody. Pollard, too, realized the conflicting nature of his priorities. At his sentencing, Pollard apologetically stated

> Unfortunately, what I failed to remember was that whenever a civil servant can no longer abide by the political constraints of the

> administration in which he serves or for whom he serves, he really only has one obligation, both to himself and the nation, and that is to resign in order to maintain his personal and his civic responsibility. (qtd. in Blitzer 252)

Pollard's case not only demonstrates the relevance of cultural assumptions and values, his actions also capture the importance of cultural artifacts such as physical and personnel security and peer reporting to the detection and prevention of security failures.

One of the most controversial artifacts of the intelligence culture is the use of polygraph technology in pre- and post-employment screening exercises. While the validity and accuracy of the polygraph as an instrument of truthfulness remains controversial, most intelligence organizations rely on this artifact to detect and develop issues that may be material to an individual's suitability for employment in the intelligence field. In Pollard's case, for example, information that surfaced during a pre-employment polygraph examination disqualified Pollard from employment consideration at the CIA. Absent that examination, Pollard might have eventually acquired access to information that was potentially more damaging to the United States's security interests than the intelligence he obtained through his ONI assignments. His handlers also realized the threat that the polygraph posed to their operation, and "Pollard was told that if he were ever picked up for questioning, he should always delay for as long as possible any polygraph examinations" (Blitzer 95).

Whereas the CIA and Israelis recognized the value of this tool, Naval intelligence apparently did not. On January 3, 1985, Pollard completed a periodic reinvestigation for continued suitability clearance that did not include the use of polygraph technology that likely would have revealed his espionage activities. Instead,

Pollard promised to abide by non-disclosure principles and signed a security agreement, another cultural artifact of the intelligence community. Afterward, his clearance level allowed access to sensitive compartmented information, or SCI, which is a heightened Top Secret clearance level for exceptionally classified information (Blitzer 95). The lack of the polygraph artifact ensured the continuation of Pollard's unauthorized collection and distribution of classified information. There were other cultural artifacts that, although they exist in the intelligence community to detect and deter security failures, were noticeably ineffective in the Pollard scenario. Of particular notoriety were physical and personnel security shortcomings as well as inadequate peer reporting mechanisms.

In 1981, Pollard assisted in establishing communications between the CIA and South African naval officials. The South Africans provided the CIA with important information on the location and abilities of various Soviet warships (Blitzer 58). Due in part to conflicts between the CIA and Naval Investigative Service, Pollard's role in the communication channel began to unravel, and questions arose concerning the veracity of his relationship with the South Africans. Of Pollard, a senior ONI official observed that "[i]t became obvious the guy [Pollard] had to be unstable" (qtd. in Blitzer 59). The official also stated that Pollard "wasn't on anybody else's wavelength," which is why "the system got nervous about him'" (qtd. in Blitzer 59). The only consequence of his peers' observations was the temporary suspension of Pollard's credentials, which the Navy reinstated after a psychological assessment administered by a friend of Dr. Morris Pollard concluded Pollard was stable. The Naval Investigative Service pursued no other investigation action on Pollard's alleged relationship with South African officials, and

in June 1984 Pollard received a transfer to the ONI's Anti-Terrorist Alert Center (ATAC).

Pollard's transfer to ATAC was not a reward for exemplary performance. Blitzer points out that when "a new unit like ATAC is created…they will very often ask those people who are considered troublemakers or nonproducers to make the switch" (Blitzer 66). The supervisory process of transferring or promoting problem employees is an issue that will resurface in the Ames survey, and the transfer of Pollard to ATAC only increased the number of classified documents to which he would obtain access. The intelligence community's personnel security procedures failed, and so would the supposed physical security measures at ATAC.

Intelligence organizations, especially those with active counterintelligence components, generally perform at least random searches of employees as they enter and particularly as they leave work environments where classified information is available. Employees also traditionally gain entrance to structures that house classified information only after presentation and verification of proper identification. Naval Intelligence, however, half-heartedly implemented appropriate security precautions and enforced no basic counterintelligence security measures. Employees were not subject to searches, and officers did not monitor whether employees requested access to classified information that they (the employees) had no need to review based on their intelligence assignments. After his assignment to ATAC, Pollard "discovered that he could easily smuggle files out of his office" (Blitzer 71). In fact, at only his second meeting with Aviem Sella, his initial handler, Pollard delivered forty-eight classified intelligence publications and photographs that he removed from ATAC without notice (Blitzer 78).

Pollard would increase gradually the number of documents he smuggled, undetected, from the ATAC, and ultimately he "delivered literally suitcases full of classified documents that he had been collecting" (Blitzer 94). Even then-Secretary of Defense Casper Weinberger, in a pre-sentencing memorandum to the court, noted that Pollard frequently acted as a courier of classified documents (Blitzer 223). It was not until Pollard's ATAC supervisor, Phillip Agee, suspected Pollard might be involved in espionage that qualified counterintelligence officers became involved in the investigation (Blitzer 228). As inadequate as the physical security lapses were, however, other personnel security shortcomings also contributed to Pollard's success at espionage.

Pollard's January 3, 1985, security review did not include a polygraph examination, and it apparently lacked a financial analysis component as well. To increase the scope and effectiveness of periodic reinvestigations, the reviews should at a minimum include a review of a subject's credit history and assets. Review of these items is a basic fixture of personnel security investigations and should always occur in security investigations. A cursory review of the Pollards' credit history would have revealed that between November 1984 and November 1985 the Pollards made payments in excess of $20,000 to an American Express credit card (Blitzer 103). Transactions in these amounts would have been obvious alarms to security and counterintelligence officers and could have prompted an immediate investigation into Pollard's unexplained affluence. Finally, Pollard's reluctance to complete background investigation forms in September 1985 triggered warning bells to Agee, Pollard's superior, and the intelligence specialist's failure to comply with basic personnel security requirements

initiated his undoing. Agee's suspicions and another co-worker's observation of Pollard leaving the ATAC with Top Secret documents led to the espionage investigation of Jonathan Pollard. Unfortunately, significant damage to the United States national security had already occurred by the time the Pollard investigation began.

Another reason that Pollard was able to conduct espionage activities undetected for an extended period of time was the necessity of the intelligence community performing its functions in a secretive manner and the little-discussed effect this secrecy has on spousal relations. This issue affects assumptions about the intelligence mission, and it also has a role in the application of cultural artifacts of an intelligence organization. A common underlying assumption is that most assignments contain classified information and, in accordance with governmental non-disclosure agreements, technically prohibit employees from discussing their duties with their spouses (unless, of course, the spouse also has the requisite clearance access and need to know). Individual values, however, frequently dictate otherwise. That is, it is not uncommon for intelligence professionals to discuss with their spouses various work assignments and personal reflections on the value of those assignments.

Pollard, for example, shared with his wife far more than details about official assignments; he also told her about his espionage plans to benefit Israel. Blitzer notes that "Anne knew all about his actions from the very start" (Blitzer 85). More troubling than Pollard's disclosure to Anne Pollard of his intentions to provide classified information to unauthorized recipients was his collection of classified documents related to the People's Republic of China (PRC). Pollard turned over to his wife substantial intelligence data on the PRC to increase the likelihood of her securing a

public relations contract with Chinese embassy officials (Blitzer 103-04). Both Pollards remained adamant that Anne Pollard never communicated the contents of these classified documents to Chinese officials, but she clearly had neither the clearance nor the need to know such information. As did her husband, Anne Pollard would also quickly learn to enjoy the fruits of the illicit proceeds her husband received from Israel. Jonathan Pollard's liberal information sharing and spousal awareness of unexplained income are other red flags that a more thorough periodic reinvestigation or counterintelligence review would have uncovered if conducted properly.

The classified information that Pollard gave and sold to Israel during his career with Naval Intelligence may have compromised crucial intelligence sources and methods, and ironically his actions weakened relations between the United States and Israel. Obviously, his espionage on behalf of Israel also had a disquieting effect on the United States's relations with various Middle Eastern states as well. Despite the negative consequences of Pollard's activities on the United States's intelligence abilities, there are positive results associated with those compromises.

Predictably, the announcement of Pollard's arrest on espionage charges prompted immediate calls for improved counterintelligence investigations of intelligence personnel. Senator David Durenberger, former chairman of the Senate Select Committee on Intelligence, issued a statement claiming Pollard's espionage "reinforces the need for immediate action on the numerous proposals for improvement in counterintelligence" (qtd. in Blitzer 185). In purely reactionary fashion, following the Pollard affair there were also calls from Justice Department officials for stricter FBI

background checks of persons of Jewish ancestry whose positions necessitated access to classified information.

Intelligence professionals and supervisory personnel should note that the Pollard espionage matter spotlighted several areas of concern for intelligence managers, security officers, and counterintelligence staff. First, ethnic diversity in the intelligence community is a necessity for the diversity of values it makes available to the organization. However, managers should be mindful that diverse values may not be welcome in homogenous work environments, and it is incumbent on supervisors to balance the need for ethnic and value diversity with monitoring of employees for behavior not consistent with the intelligence community's basic underlying assumptions. Second, intelligence managers, in concert with counterintelligence staff, must ensure that adequate physical and personnel security measures are in place to deter if not detect threats to operational security. Such countermeasures include polygraph applications, heightened physical security precautions, and improved background investigations of intelligence employees and their spouses. Third, intelligence agencies should implement better mechanisms for peer and spousal reporting of suspicious activities by intelligence employees. Intelligence organizations should request greater flexibility for dealing with internal personnel issues such as poor performance. Agencies must be able to deal with problem employees without promoting the individual or merely transferring the person to another area within or without the organization. Fourth, intelligence leadership must balance the needs of the agencies with the missions of the organizations and rights of individual employees. Intelligence managers would do well to realize operational threats are omnipresent, but proper

internal safeguards can prevent organizational culture principles from contributing to security failures.

CHAPTER FIVE
AMES CASE STUDY

On February 21, 1994, Aldrich Hazen Ames departed his suburban residence outside Washington, D.C., in Arlington, Virginia. Ames's commute that day was to be like no other. Shortly after leaving his residence, FBI agents stopped Ames's vehicle and arrested him on charges of conspiracy to commit espionage for Russia and its predecessor state, the former Soviet Union. The arrest of Ames effectively ended one of the most devastating penetrations of the United States intelligence system by a foreign power. The magnitude of Ames's espionage activities and their impact on the United States's intelligence sources, methods, and past assessments of Soviet abilities and weaknesses would not become known until months after his arrest. Investigators did know by the time of his arrest that Ames provided the Soviets and then Russians with some of the CIA's most classified intelligence, and the information he provided was directly responsible for the death or imprisonment of as many as thirty sources of the CIA and FBI.

On April 28, 1994, Aldrich Ames and his wife, Rosario Ames, pled guilty to charges based on their espionage activities. In exchange for their guilty pleas and promised cooperation with intelligence and law enforcement authorities, Aldrich Ames received a lifetime prison sentence, and his wife received a sentence of sixty-three months in prison (Senate Assessment 4). Rosario Ames has completed her sentence, but Aldrich H. Ames, prisoner number 40087-083, is currently serving his sentence for life at the Allenwood federal penitentiary near White Deer, Pennsylvania.

At the time of his arrest, Ames had been an employee of the CIA for 31 years, and he spent practically his entire career in the CIA's clandestine Directorate of

Operations (DO). The security classification of information to which he had access was routinely Top Secret/SCI, and it included the names and identities of United States agents and double agents abroad and within the United States. Particularly devastating was the fact that Ames had immediate, unquestioned access to the information most desired by the Soviets and Russians. Ames provided his handlers with damaging national security information for almost ten years, and a review of the Ames affair demonstrates that numerous organizational culture principles specific to the intelligence community contributed to this unprecedented security failure. The most prominent organizational factors in the Pollard affair were also problems in the Ames case. In addition to employee motivation issues and physical and personnel security requirements, the affair also included an extreme inadequacy of information-sharing protocols. The depth of Ames's espionage activities dictate a categorical approach to an assessment of culture's impact on the Ames security failure. An overview of his familial and educational background as well as career progression is also insightful.

Aldrich "Rick" Ames's introduction to the intelligence community mirrored Jonathan Pollard's experiences. Ames's father, Carleton Ames, held a doctorate degree and began working for the CIA's DO in 1952. Carleton Ames and his family completed an overseas tour in Southeast Asia by 1955, and due in part to his alcohol abuse and poor performance ratings, Carleton Ames spent the remainder of his career at CIA headquarters (Senate Assessment 5). Several years later, in 1960, Aldrich Ames would begin a CIA career that amazingly would mirror his father's employment journey.

Ames first worked for the CIA as a painter in 1960, and he later found employment as a clerk typist on a full-time basis. Ames worked for the CIA as a

document analyst in the DO for the next several years while he pursued a bachelor's degree in history at George Washington University. Ames subsequently applied to the CIA's Career Trainee Program and entered training for the clandestine service in 1967 (Senate Assessment 6). His first overseas assignment was in Ankara, Turkey, and supervisory appraisals of his performance "considered him unsuitable for field work and expressed the view that perhaps he should spend the remainder of his career at CIA headquarters in Langley" (Senate Assessment 7).

Ames's next assignment was, in fact, a headquarters rotation, which was followed by assignments in New York City. Despite numerous security infractions that should have raised suitability concerns, Ames enjoyed enthusiastically positive performance appraisals from his supervisors during these assignments and ultimately received promotion(s) to a GS-14 pay grade. Ames's successes, however, would be short-lived, and his next assignment to Mexico City reinforced previous appraisals of Ames's inability to function adequately in an overseas recruitment environment. In fact, "Ames appeared stronger handling established sources rather than developing new ones" (Senate Assessment 9). While assigned to Mexico City Ames began an extramarital affair with Maria de Rosario Casas Dupuy, a paid CIA source, and she afterwards relocated to join Ames, whose next assignment at CIA headquarters was as counterintelligence branch chief for Soviet operations in the DO.

Ames's headquarters assignment was in Soviet counterintelligence, and he also assisted a field office whose function was source development in the Washington, D.C., area. Due to his counterintelligence duties, "Ames was in a position to gain access to all CIA operations involving Soviet intelligence officers worldwide" (Senate

Assessment 11). In addition, "[h]is assignment also gave him access to all CIA plans and operations targeted against the KGB and GRU intelligence services" (Senate Assessment 11). Ames served in this position until his voluntary transfer to Rome from 1986 to 1989, and once again, Ames's performance evaluations reflected negatively on his abilities. Despite poor appraisals and a record of committing flagrant security violations, Ames returned to the DO's Soviet Operations Division in 1989 and later was transferred to the Counterintelligence Center Analysis Group and Counternarcotics Center where he remained until his arrest in February 1994 (Senate Assessment 42-44). In each of his assignments Ames exhibited behavior inconsistent with intelligence organizations' expectations of its employees. He routinely violated security rules, placed himself in compromising situations, and he contradicted the basic assumptions of intelligence work as well as the values that shape its conduct.

Unlike Jonathan Pollard, whose motivation to commit espionage supposedly did not include financial gain initially, Aldrich Ames's only incentive to commit espionage was the possibility of monetary rewards. Ames's reasons for disclosing classified information to unauthorized sources were completely self-serving and fit Downs's model of a careerist climber whose personal gain eclipses all other concerns (Thomas 400). Ames recalled that financial difficulties caused him first to consider espionage in late 1984 or early 1985. Ames had personal debts from his recent divorce settlement, a car loan, a signature loan, credit card payments, and other expenses associated with Rosario's arrival in the United States. Ames stated that "[i]t was these pressures…which in April 1985, led him [Ames] to conceive of 'a scam to get money from the KGB'" (Senate Assessment 14). Ames's espionage activities might have been

prevented, however, had intelligence artifacts such as personnel security measures, peer reporting mechanisms, and supervisory oversight been more proactive.

Certain behaviors weaken employee credibility and suitability at a minimum and jeopardize intelligence operations at the other extreme. Ames's career is replete with security infractions that should be outright intolerable in the intelligence community. While assigned to New York, Ames left a briefcase full of classified information on a subway train, and he also received a citation for not securing various Top Secret communications equipment. Neither action resulted in any reprimand or corrective action. He also brought Rosario to a secure apartment in New York provided by the CIA and occasionally used his personal computer to prepare classified documents (CIA OIG Abstract 19). Ames also reportedly removed from CIA headquarters plastic bags containing "five to seven pounds" of classified information (CIA OIG Abstract 20). While in Mexico, Ames had at least three extramarital affairs that he did not report, and neither he nor his coworkers reported his involvement with Rosario Dupuy, a foreign national known to be on the CIA's payroll (CIA OIG Abstract 20). The DO tendency to protect its own prevailed. Other peers of Ames stated that Ames "frequently showed interest in areas unrelated to his immediate area of responsibility" (Senate Assessment 28). However, "none of those colleagues ever made this a matter for the record" (Senate Assessment 28). In one glaring example of failed peer reporting requirements, the following information surfaced regarding Ames's contact with Soviet officials:

> One of Ames's subordinates in Rome told the FBI after Ames's arrest that she had suspected Ames was not fully documenting the relationship between himself and the Soviet official. In fact, she had searched the office data base to see whether Ames was reporting all of his contacts. Although she concluded that he was not, she did not notify any senior manager. (Senate Assessment 29)

All of Ames's security violations belied the basic assumptions that form the foundation of an intelligence organization's culture, and organizational artifacts that could have decreased the severity of the Ames affair were noticeably absent.

During his Mexico assignment, Ames also began to abuse alcohol. His problem drinking resulted in recommendations that he receive treatment for alcohol abuse upon return to headquarters. Ames "had one counseling session but there was no follow up program of treatment" (Senate Assessment 10). Several Agency personnel who supervised Ames did not report his behavior because "alcohol abuse was not uncommon in the DO during the mid- to late-1980s," and other managers pointed to a lack of support from Langley in dealing with employees who represented problems or threats to CIA objectives (CIA OIG Abstract 20-21). The DO's protective posture reinforced this trend. One report concluded that a DO officer "who has been through training, gone through the polygraph examination, and had an overseas assignment, is accepted as a 'member of the club,' whose fitness for assignments, promotions, and continued service becomes immune from challenge" (Senate Assessment 70).

Reminiscent of Pollard's transfer to the ATAC as a managerial means of dealing with someone whom supervisors considered a problem employee, CIA headquarters personnel adopted similar procedures to deal with Ames. Ames's transfer to Rome from Langley reportedly "was seen as a good way to move a weak performer out of headquarters" (Senate Assessment 27). Ames's alcohol abuse was only one of several personnel security issues that peers and supervisors should have reported for proper application of artifacts of the intelligence culture. Ames's unexplained wealth, spending habits, foreign travel, and acquisitions, for example, were certainly not in line

with most other intelligence professionals' abilities and should have alerted counterintelligence officers also.

Ames's supervisors noted that he received frequent counseling for failure to submit timely reports and financial accountings of operational fund disbursements (CIA OIG Abstract 18-19). These failures complemented Ames's existing reputation for administrative weakness as evidenced by appraisals that noted his "tendency to procrastinate, particularly in terms of his late submissions of his financial accountings and operational contact reports" (Senate Assessment 8). Ames's operational finances, however, were only a smaller part of a much larger financial problem. His personal finances were a model case study in the undue affluence counterintelligence officers should look for when conducting periodic reinvestigations or security inquiries.

Ames received his first payment from the Soviets on May 17, 1985. According to Ames, the initial $50,000 that he received was to be a "one time deal" (Senate Assessment 16). It was not a one time deal, however, as Ames received approximately $2.5 million for the information he sold, and the proceeds he derived from this conduct allowed considerable purchase power. While receiving an annual salary of less than $70,000, Ames managed to purchase new Jaguar automobiles and a home—for which he paid cash—valued at $540,000 (Senate Assessment 2). Ames explained his newfound wealth by claiming that Rosario Ames's wealthy family had provided financial assistance to the couple. However, more extensive investigations would have revealed the deception behind Ames's explanations (CIA OIG Abstract 22-23). Additionally, proper application of polygraph technology also would have limited the security compromises Ames committed.

Prior to departing for Rome in 1986, Ames learned that he would have to complete a polygraph examination before his European assignment began. Ames later revealed that he "might not have made the decision to commit espionage in April of 1985 if he had known that he was going to be polygraphed the next year" (Senate Assessment 26). After Ames's arrest, the FBI review of Ames's polygraph results revealed unresolved questions about Ames's apparently deceptive responses to counterintelligence questioning. The FBI determined that had the CIA polygraphers did not apply the instrument properly and should have developed more detailed questioning based on Ames's responses to initial questions (CIA OIG Abstract 26-27). The 1986 examination was not Ames's only polygraph experience.

In 1991 Ames again underwent a background investigation (including financial review) and polygraph testing. Although the background investigation and financial scrutiny raised questions about Ames's suitability for access to classified information, the polygraph examiners who conducted the 1991 examination did not receive those investigative results before they conducted the polygraph tests. The examiners noted that "having such detailed information available could have significantly altered their approach to testing Ames" (CIA OIG Abstract 27). Better information sharing could have improved the quality of the polygraph examination and may have detected Ames's activities sooner. This miscommunication is merely a minor snapshot of the problems inherent in the intelligence community's guarded information sharing and the effect that such mutations of the assumption have on operational security.

Former Inspector General Hitz succinctly summarizes the impact of the information sharing assumption when he argues that "the major failing in the Ames case

appears to be traceable to non-coordination and non-sharing of derogatory information concerning Ames" (Hitz 26). In addition, "Hitz elaborated on this by concluding that the Ames case resulted from 'ambiguous divisions of responsibility,' 'breakdown in communication,' and an 'absence of collaboration and sharing of information'" (qtd. in Turner 260). Hitz's reference is to both the CIA's internal compartmentation structure that prevented information sharing across divisions, and the Agency's unwillingness to share information with its FBI counterparts who have the responsibility for domestic espionage investigations.

As early as 1986 the CIA had established an investigative group to determine the reason(s) for various source and operation compromises:

> The CIA IG report indicates that the investigation group was hesitant to solicit financial expertise from other components within CIA, such as the Office of Financial Management or the IG Audit Staff, and that they were even more wary of seeking help from any outside sources such as the FBI. They felt that people outside of the Directorate of Operations would not have the proper sensitivities to the DO Culture or to the fact that CIA employees were under scrutiny. (Senate Assessment 53)

Finally, in mid-1991, the joint CIA/FBI investigation of the compromises began as the Special Investigations Unit (SIU). The group included two CIA counterintelligence experts, an FBI agent, and an FBI analyst (DOJ OIG Review C). While the CIA leadership suspected as early as 1986 that a CIA officer might be responsible for the significant security compromises the Agency suffered, the CIA did not formally advise the FBI of the specific case details until 1993. In fact, even after the creation of the SIU, "FBI members of the SIU were given full access to the information that had been developed concerning Ames…[t]hey had almost no involvement in the investigation of Ames" (DOJ OIG Review C). The CIA initially dismissed the possibility of an Agency

penetration being responsible for the compromises, and the intelligence : law enforcement ideological differences referenced earlier prohibited the free exchange of information that would have identified Ames as the CIA mole years in advance of 1991 when Ames appeared as one of twenty-nine employees suspected of compromising Agency operations.

The trend of managerial inattentiveness to substandard performance, undesirable behavioral patterns, and the security threats associated with these issues are recurrent themes in the intelligence organization culture. As noted by former Inspector General Hitz's report on the Ames affair,

> Although information regarding Ames's professional and personal failings may not have been available in the aggregate to all of his managers or in any complete and official record, little effort was made by those managers who were aware of Ames's poor performance and behavioral problems to identify the problems officially and deal with them. If Agency management had acted more responsibly and responsively as these problems arose, it is possible that the Ames case could have been avoided in that he might not have been placed in a position where he could give away such sensitive source information. (CIA OIG Abstract 11)

Supervisory assumptions trumped organizational assumptions in the context of the Ames case. The Agency's most critical shortcomings were in its system of artifacts, as they were unable to address the threat posed by a disgruntled employee with a rapidly-declining value system whose environment lacked adequate operational safeguards. The CIA's hesitance to share information with law enforcement represents a mutation of a core underlying assumption of the intelligence culture and is largely to blame for the massive security failure.

Despite the obvious negative results of Ames's espionage activities, one positive consequence was that the intelligence community and its leadership identified numerous

areas for improvement and implemented several programs to improve organizational efficiency and minimize the risk of security breaches. On May 3, 1994, former President Clinton issued Presidential Decision Directive (PDD) 44. The counterintelligence directive's intent was "to foster increased cooperation, coordination and accountability among all US counterintelligence agencies" (White House "U.S. Counterintelligence Effectiveness"). PDD 44 also created the National Counterintelligence Center as an information clearinghouse and requires improved information exchanges between FBI and CIA managers to achieve better law enforcement : intelligence coordination (White House "U.S. Counterintelligence Effectiveness"). The directive reinforces the existing requirements for information sharing originally specified in Executive Order 12333 and a 1988 memorandum of understanding between the FBI and CIA. To facilitate improved information exchange, the directive "placed a senior FBI official in charge of counterespionage inside CIA headquarters" (Kitfield "Anti-terror"). Such a placement and cooperation would not have occurred prior to Ames's arrest.

In the aftermath of the Ames case, Justice Department and Agency officials have cited increased levels of cooperation for the identification and neutralization of other security threats such as those posed by Harold Nicholson, the former CIA station chief in Romania. The FBI arrested Nicholson on November 16, 1996, for violating Title XVIII, section 794, or committing espionage and conspiracy to commit espionage on behalf of Russia (CIA Joint Press Release). Whereas the Ames affair revealed startling miscommunications within and outside the CIA about Ames's polygraph results and background investigations, in the Nicholson case, "the deception and

Nicholson's behavior immediately triggered a counterintelligence investigation, and the FBI was informed up front about a potential spy case" (Hulnick 280). In a press release issued by the CIA after Nicholson's arrest, then-Director of Central Intelligence John Deutch observed:

> The arrest of Nicholson is the direct result of an unprecedented level of cooperation between the CIA and the FBI. We are now able to demonstrate quite conclusively that the post-Ames reforms worked as designed. Clearly the post-Ames analysis and detection mechanisms the CIA and FBI put in place succeeded in the identification of Nicholson and his alleged espionage activities on behalf of the Russian intelligence service. (CIA Joint Press Release)

Commenting on Nicholson's arrest on espionage charges, former FBI director Louis Freeh echoed DCI Deutch and stated that the "most formidable weapon against this grave crime is a close partnership between the FBI and the CIA" (CIA Joint Press Release). The leaders' statements reflect their attempts to reconcile conflicting ideologies and cultural assumptions applicable to the entire intelligence community.

Improved FBI : CIA cooperation is largely attributable to the efforts of senior Agency and Bureau officials known as the "Gang of Eight" (Hulnick 282). These senior leaders have recognized the need to establish firewalls between law enforcement and intelligence so that communication between them does not jeopardize sources, methods, or other operational concerns specific to each agency. The CIA's lead representative to the Gang of Eight meetings was then-Deputy Director George Tenet. Addressing the importance of this group and its efforts, DCI Tenet commented

> I think the Ames case was the jumping off point in taking cooperation between the FBI and CIA seriously, because it proved that we could no longer tolerate petty bureaucratic jealousy and turf wars in dealing with threats to American security. And from the very beginning, we consciously sought to institutionalize the reforms at all working levels so

> that they would become steeped in our culture and not dependent on transient personalities. (qtd. in Kitfield 2868)

In observance of the necessity to bridge the gaps in intelligence and law enforcement cooperation without ruffling existing cultural assumptions or ideologies, Congress passed the Intelligence Authorization Act of 1996. The Act permits the FBI "to task both the CIA and NSA to gather intelligence against targets related to FBI cases" (Hulnick 275). This statutory requirement imposes stricter standards on both intelligence and law enforcement and likely will result in improved threat assessments, criminal prosecutions, and, optimistically, prevention of grand-scale security failures and terrorist attacks. The intelligence : law enforcement divide is primarily ideological; they share numerous cultural assumptions and should strive to prevent exaggerations of assumptions and employ cultural artifacts in a manner consistent with organizational requirements for security. Successful applications of these principles resulted in the arrest of Harold Nicholson, and they were also instrumental in the detection of FBI special agent Robert Philip Hanssen's espionage activities and subsequent arrest for those crimes.

CHAPTER SIX
HANSSEN CASE STUDY

On February 18, 2001, agents of the Federal Bureau of Investigation armed with a search warrant and an arrest warrant arrived at a park outside Vienna, Virginia. Agents had previously drafted an affidavit in support of the arrest of an individual believed to have committed espionage against the United States. The investigators also had permission to search a single-family residence located at 9414 Talisman Drive, Vienna, Virginia. FBI agents sought to search the premises and arrest an occupant of the Vienna residence for violations of Title XVIII United States Code, Sections 794 (a) and 794 (c). Specifically, the warrant for arrest alleged that its subject had transmitted national defense information without authorization and conspired to commit espionage against the United States (FBI Affidavit par. 4). National security investigations and arrests for criminal conduct associated with such affairs are everyday occurrences for the FBI since that agency has primary enforcement authority for those alleged crimes. It is not common, however, for the FBI to arrest one of its own. On February 18, however, FBI agents arrested special agent Robert Philip Hanssen, a twenty-five year veteran of the FBI, for committing espionage on behalf of the Soviet Union and Russia since 1985.

Hanssen's arrest sent shock waves throughout the law enforcement and intelligence community. Counterintelligence officials were especially startled by the revelations that Hanssen, a seasoned FBI agent with extensive experience in counterintelligence operations, had allegedly been on the Soviet and Russian payrolls since 1985. Later confirmation of these allegations confirmed that Hanssen had been a Soviet spy for fifteen of his twenty-five years as an FBI agent, and Hanssen's defense

attorney later announced that Hanssen began spying as early as 1979 ("Hanssen"). The consequences of Hanssen's actions were devastating to intelligence and law enforcement agencies whose missions involved the collection, analysis, and investigation of national security information and suspected compromises thereof. The enormity of the damage to national security caused by Hanssen's compromises would not be known until CIA and FBI personnel debriefed Hanssen following his guilty pleas.

On June 14, 2001, the Department of Justice submitted for legal consideration a plea agreement between the United States and Robert Philip Hanssen. The plea agreement Hanssen entered into with the government acknowledged Hanssen committed "13 counts of substantive acts of espionage and one count of attempted espionage" on behalf of foreign powers, namely the former Soviet Union and Russian Federation (DOJ "Hanssen"). The agreement also required Hanssen's unfettered cooperation with law enforcement and intelligence officials so they may "assess the full scope and consequences of Hanssen's espionage activity, and the damage he has caused his country" (DOJ "Hanssen"). By pleading guilty, Hanssen avoided a possible death sentence for his crimes but is ineligible for parole.

Like Pollard and Ames, whose childhood and adolescent exposure to the intelligence field influenced their career choices, Robert Philip Hanssen's father was a veteran lieutenant for the Chicago Police Department in Chicago, Illinois. Hanssen's familiarity with the law enforcement community undoubtedly influenced his decision to pursue a career in law enforcement. Like Pollard and Ames, Hanssen acknowledged an early interest in intelligence issues. On or about March 14, 2000, Hanssen (also known

as “B” to his Russian handlers), prepared a letter in which he stated, “I decided on this course when I was 14 years old” (FBI Affidavit par. 130). For Hanssen, however, the motivation to commit espionage was not a straightforward financial reason as it was for Ames. Like Pollard, Hanssen’s motives for his actions were mixed, and the FBI agent’s education, training, and career progression influenced his values and motivation for committing espionage. These factors also enabled Hanssen to remain undetected for fifteen years.

Hanssen received an AB degree in chemistry from Knox College in 1966. After studying dentistry for approximately two years, Hanssen earned an MBA in accounting and information systems from Northwestern University in 1971. He became a certified public accountant (CPA) in 1973 after working for two years as a junior accountant. Prior to passing the CPA examination Hanssen entered on duty as an investigator with the Financial Section of the Chicago Police Department’s Inspection Services Division (FBI Affidavit par. 23-24). In January 1976 Hanssen began his career as a special agent with the Federal Bureau of Investigation, a position he retained until his arrest in February 2001.

Upon completion of his initial FBI training, Hanssen worked on a white-collar crime squad in Gary, Indiana until 1978. He then transferred to the FBI field office in New York, New York, and his assignments concentrated on criminal accounting practices and investigations. Beginning in March 1979, Hanssen assisted with the New York Field Office’s development of an automated counterintelligence database and obtained access to information on intelligence officers and other foreign officials assigned to the United States (FBI Affidavit par. 26-29). From 1981 to 1985 Hanssen

served as a supervisor in the Intelligence Division of FBI headquarters. He also worked in the FBI's Budget Unit and obtained access to detailed information on FBI sources and counterintelligence activities. Between 1983 and 1985 Hanssen worked in the Bureau's Soviet Analytical Unit and Foreign Counterintelligence (FCI) Technical Committee (FBI Affidavit par. 30). Hanssen enjoyed frequent assignments in Washington, D.C., and New York, New York, where his duties focused primarily on Soviet intelligence and counterintelligence operations. He also spent six years as a senior FBI counterintelligence representative at the Department of State. Hanssen's numerous assignments in the Bureau's intelligence and operations divisions necessitated ongoing training in counterintelligence tradecraft. While the specific training Hanssen received is classified, it is common knowledge that the instruction he received better prepared him for the rigors of espionage.

By all accounts, Hanssen's counterintelligence and information systems training prevented earlier detection of his involvement with the Soviets and Russians. He also was cautious not to exhibit behavior that might alert his peers, superiors, or counterintelligence officers to his actions. During the periods where Hanssen spied for foreign governments and received substantial payments for the information he supplied, Lawrence Walsh notes that he "displayed no signs of extravagance…maintained his purist, church-going lifestyle…exhibited exemplary diligence in his professional duties, ingratiating himself to his superiors" (Walsh n.p.) Pollard and Ames became careless about their activities, but Hanssen was cautious not to attract attention to himself and proactively sought to discourage suspicions that he might be a spy. Whereas Pollard and Ames allowed financial gain to corrupt them, Hanssen's self-proclaimed motives

for espionage were not financial. As former DCI James Woolsey noted, his "personality and his arrogance had something to do with his decision" to commit espionage (Woolsey n.p.). Hanssen committed espionage to pacify his ego, and that motivation creates difficulties for investigators because value-based threats are less apparent and more complex to detect than other (i.e., financial) incentives to commit espionage.

Despite Hanssen's exemplary performance in all of his FBI assignments, he did not receive appointments to senior positions. Although he was proficient in his duties and regarded well by supervisors, Walsh notes that Hanssen "was passed over several times for command positions, instead being placed on desk jobs" (Walsh n.p.). He notes that Hanssen's failure to receive promotions made him (Hanssen) feel indignant (Walsh n.p.). Walsh also references one commentator who noted that "Hanssen betrayed his country to feed a more basic need: to pump up his ego" (qtd. in Walsh n.p.). Former FBI profiler Bill Tafoya observed that "[w]hen we sense that somebody is not appreciating us, someone is either ignoring or, worse, criticizing us, our self-worth is challenged" (qtd. in Walsh n.p.).

Tafoya also suggests that Hanssen and other "ego-driven insiders are motivated more by the trophies they collect for themselves than the acknowledgement of others…. As long as he remained one step ahead of internal security, Hanssen could bask in the self-knowledge that he was better than so-called superiors" (qtd. in Walsh n.p.). According to Walsh, what made Hanssen more dangerous than others is that he "cultivated the trust of his superiors…internalized his frustration and directed his skills and knowledge to a nefarious pursuit" (Walsh n.p.). By remaining below the

counterintelligence radar, Hanssen avoided cultural artifacts inherent in the intelligence community. His actions also undercut basic assumptions about intelligence by satisfying his own individual value needs.

One of the flawed basic assumptions in intelligence organizations that Hanssen leveraged to his advantage is the errant belief that personnel who occupy senior intelligence positions are immune from the influence(s) of espionage. Individuals with considerable experience and training are perceived frequently as lesser threats than agents or field operatives who have routine access to other states' intelligence representatives. The high level of trust imparted to senior professionals is necessary in the intelligence community, but the assumption that employee value systems are always consistent with the organizations' values is unrealistic. Consider, for example, the extent to which Hanssen abused this assumption in furtherance of his crimes.

Hanssen's placement in senior level FBI positions necessitated access to highly compartmented information. There was a blanket assumption that, based on his duties and responsibilities, Hanssen's need to know classified information was unquestionable. He routinely accessed the FBI's computer systems to determine whether he was "the subject of FBI investigative interest, including checking FBI records to determine whether there have been recent entries as to his own name, his home address, or the signal site" Hanssen used to communicate with his handlers (FBI Affidavit par. 5f).

Another impediment to operational security that is traceable to a flaw in the basic underlying assumptions in the intelligence community is the tendency for individuals who amass significant experience in a given subject area to be considered indispensable to a specific function. Persons considered to possess special skills are

less likely to rotate out of positions where their continued exposure to certain intelligence increases the risk that the information could be compromised. Frequent reassignments and rotations of key personnel prevent extensive exposure to classified information and represent another cultural artifact that, when implemented, may forestall security failures. Better application of this cultural artifact, in conjunction with improved polygraph testing, is important to improving operational security.

Unlike the CIA and other intelligence organizations, the FBI has not required polygraph examinations of agents during periodic background reinvestigations. The Bureau utilizes the polygraph as a pre-employment screening tool, but its post-employment application has been limited historically to the examination of sources of information and suspects. The noticeable absence of the polygraph within the FBI as a deterrent to espionage or any other crime for its agents is a critical cultural shortcoming that is inconsistent with an assumption that intelligence professionals maintain the highest degree of integrity and honesty. In the Pollard case and Ames affair, despite concerns over its accuracy and legitimacy, the possibility of polygraph examination represented a significant threat to continued espionage activities. Although Ames's espionage efforts continued after he underwent polygraph testing, better administration of the exam and improved information sharing about his results could have revealed his actions much earlier. The application of polygraph technology in Hanssen's case could have minimized the damage he caused also.

Fortunately, once the Bureau determined the existence of a security breach within its ranks, the FBI's investigation of Hanssen did not suffer from interagency turf battles common in task forces formed to investigate serious crimes. Intelligence and

law enforcement cooperation were much improved in this case than relations had been during the Ames affair. At the time of Hanssen's arrest, Louis Freeh was the director of the FBI.

> Freeh said the investigation that led to the charges is a direct result of the combined and continuing FBI/CIA effort ongoing for many years to identify additional foreign penetrations of the U.S. intelligence community. The investigation of Hanssen was conducted by the FBI with direct assistance from the CIA, Department of State and the Justice Department, and represents an aggressive and creative effort which led to this counterintelligence success. (FBI Statement)

There is also no evidence that supervisory complacency contributed to Hanssen's continued criminal activity. Hanssen did not receive promotions as a means of dealing with an agent his supervisors considered eccentric. Once the investigation into Hanssen's espionage began, investigators reconstructed Hanssen's assignments and contacts he had in each of his assignments. Despite Hanssen's attempt to conceal large monetary payments from his handlers, FBI agents conducted thorough financial reviews that determined Hanssen received over $1.4 million in cash and diamonds from his espionage sponsors. Although Hanssen utilized extensive counterintelligence skills to elude suspicion, it appears from the evidence gathered that FBI agents appropriately employed various cultural artifacts to reduce the risk Hanssen posed.

The Bureau's physical security measures such as personal and electronic surveillance allowed the agency to monitor Hanssen's travels and communications with the Soviets and Russians. The technical security options they exercised included electronic and other monitoring of Hanssen's access to automated information that could have disclosed the Bureau's suspicions of him. Unfortunately, the Bureau only instituted such screening tools after it began the Hanssen investigation. The FBI also

recognized that Hanssen's counterintelligence experience and access to classified information were unnecessary risks and modified his responsibilities without alerting him to the agency's investigation. The FBI's application of the aforementioned cultural artifacts demonstrates succinctly the impact that proper and timely application of the principles can have on security compromises.

The investigation of Robert Philip Hanssen's espionage activities and his arrest for those crimes also indicate that despite their ideological differences, it is possible for law enforcement agencies with shared cultural assumptions, values, and artifacts to cooperate and supplement each other's intelligence and enforcement functions. Hanssen's guilty plea is a testament to the success of that improved coordination. The Hanssen case clearly illustrates the constructive attributes of positive cultural assumptions such as information sharing principles, and it also highlights the threat that individual values pose to operational security. The review of Hanssen's activities also imparts the importance of cultural artifacts to agencies' continued ability to identify those persons and institutions that represent the greatest danger to the United States's national security interests. Although the Hanssen study undoubtedly exhibits positive results of effective organizational culture icons of the intelligence community, there remains considerable room for improvement to the organizational culture of the United States intelligence establishment. Intelligence professionals and managers would do well to give due consideration to the observations that follow.

CHAPTER SEVEN
CONCLUSIONS AND RECOMMENDATIONS

The organizational culture of the intelligence community is unique from that of other governmental institutions and notably dissimilar from most private sector enterprises. Despite some ideological differences between intelligence agencies and law enforcement organizations, they do share numerous cultural assumptions, values, and artifacts. The cultural elements that intelligence and law enforcement share are certainly responsible for many of the security weaknesses and failures that have beset the intelligence (and to a lesser extent) law enforcement community. The case studies of Jonathan Pollard, Aldrich Ames, and Robert Hanssen demonstrate that these cultural attributes are present in the defense, intelligence, and law enforcement organizations that have intelligence collection and analysis functions. This study also concludes that cultural factors sometimes affect negatively operational security whether the cultural elements are active (i.e., assumptions) or absent (i.e., artifacts). The forces that threaten the intelligence culture's basic underlying assumptions are individual values, and organizational abilities to address this threat are extraordinarily dependent on the intelligence community's artifacts.

How, then, may intelligence organizations protect themselves from the threats that individual values systems pose to security? Walsh questions, "How do you prevent another Robert Hanssen from being cultivated by a foreign power?" (Walsh n.p.). He accurately answers that "[i]n a democratic society, the simple answer is you can't….[l]oose controls create a greater probability of exploitation, while extremely tight security alienates the people you want to trust" (Walsh n.p.). Threats to the United States intelligence infrastructure are omnipresent. Despite the most efficient application

of proactive counterintelligence measures, there will always be some degree of incompatibility between organizational assumptions and the values of those that comprise the group. What exacerbates this problem in the intelligence community is the fact that the employee training necessary to conduct intelligence responsibilities also has the unintended consequence of equipping the potential spy with skills that make detection of such efforts more difficult. Intelligence professionals and managers can only ensure that they recognize the risk posed by the nature of their operations and assets (human as well as non-human). They must also adopt proactive problem-solving approaches that deter deviation from established value systems, and they must install countermeasures that detect security weaknesses or failures. This process begins with a re-examination of the most basic assumptions of the intelligence community.

The reliability of the intelligence community is dependent on the integrity of its employees. One assumption about the intelligence profession is that those who pursue it as a career have only the noblest of intentions and will respect the secrecy requirement that is also assumed applicable at all times. Another accepted necessity is the need to limit information access through imposition of need-to-know principles and extensive compartmentation. Information sharing is extremely limited, yet the lack of adequate communication within and among agencies may also have unintended, negative consequences. Related to these processes are understandings that organizations will employ cultural artifacts in support of these assumptions. It is also understood that intelligence organizations must conduct some affairs clandestinely in order to obtain the information necessary for analysis and subsequent use by policy makers to make national security decisions. Unfortunately, a corollary assumption of

the intelligence community from without more so than within is that intelligence organizations disrespect civil liberties, moral standards, and ethical norms in furtherance of goals that are not necessarily consistent with the idealism that the organizations represent. These assumptions about the United States intelligence community must contend with individual values that challenge their validity.

The intelligence community depends on the diversity of values its employees represent. While ethnic diversity issues are not central to the espionage cases of Pollard, Ames, and Hanssen, the intelligence community would do well to stress ethnic diversity in its recruitment efforts to prevent mirror-imaging tendencies and improve the intelligence product the community creates. As Callum points out, ethnic diversity may present challenges to cultural assumptions, but homogeneity "will only perpetuate the mistakes of the past and create the failures of the future" (Callum 39). Callum also notes that "[t]he most fundamental way of improving intelligence is to establish the heterogeneity" of the intelligence community (Callum 39). Intelligence agencies should seek ethnic diversity without the use of recruitment quota systems that sacrifice quality standards in favor of quantity requirements.

Employee motivations lie at the heart of value conflicts with organizational assumptions. Intelligence agencies should attempt to create environments in which intelligence professionals may achieve self-actualization through satisfaction of monetary needs as well as fulfillment of higher level social and ideological requirements. Policy makers, in consultation with intelligence leaders and human resource managers, should ensure compensation parity exists between civil servants and the private sector. Intelligence executives should also ensure all personnel, especially

managers, receive more training and instruction in leadership skills. The United States Commission on Roles of the Intelligence Community argued that "[t]raining should be treated as a continuous part of career development at all levels and should be used to inculcate goals and values as well as develop management skills" (United States Commission). Agencies must also monitor closely employee exposure to classified information and regularly rotate intelligence staffers to minimize security vulnerabilities created by extended assignments to sensitive positions.

Intelligence agencies' stress on the importance of loyalty and integrity as personal attributes oftentimes prevent employees from reporting the suspicious behavior of peers. Organizations must encourage employees to report behavior that appears to dissent from standards expected of intelligence professionals. Intelligence managers have a corresponding duty to act on those reports and not address the complaint by recommending the transfer or promotion of potential problem employees. In the most severe cases, intelligence organizations should have greater flexibility to terminate employees whose behavior or poor performance increases their vulnerability to manipulation by other intelligence services. Agencies must also be cautious, however, to ensure such personnel removals are justifiable, as employee retribution for unwarranted dismissals may also affect security concerns negatively. Organizations should also encourage employee reporting to Office of Inspector General (OIG) staff when concerns over supervisory inattentiveness are material. The OIG, in turn, must have the authority to report directly to the executive and legislative officials any matters that the OIG believes are best addressed above the organizational level.

In recognition of the security risks that individual values represent to organizational assumptions, intelligence agencies must develop and implement cultural artifacts to enable appropriate systems of checks and balances that the intelligence mission demands. Among the artifacts to be strengthened are thorough periodic reinvestigations that include detailed financial analyses and interview of coworkers, peers, spouses, and acquaintances. Intelligence agencies should also improve physical security mechanisms to include random searches of employees and their work areas and surveillance of areas where classified information is received and analyzed. Counterintelligence and information technology experts should also remove from computer equipment any medium that allows the transfer of information from the computer to an external device (i.e., diskettes or digital discs, ethernet cards, magnetic drives, etc.).

Intelligence organizations should also emphasize the use of polygraph examinations as a counterintelligence tool. Polygraph examiners should work in concert with background investigators to ensure that derogatory information obtained in either process is made available to the other party. In his Senate Judiciary Committee testimony, former CIA counsel Jeffrey Smith points out that the polygraph remains "only one tool in an effective counterintelligence program" despite concerns over its reliability (Smith n.p.). As pointed out by Senate Intelligence Committee Chairman Richard Shelby, polygraph examinations will not "stop everything such as spying, espionage, but it will thwart a lot of it" by virtue of its deterrent effects (Shelby n.p.).

In the aftermath of numerous espionage cases, including those of Pollard and Ames, the executive and legislative branches of the United States government have

sought to implement proactive approaches to deter, detect, and respond to the threat of espionage. Their proposal to achieve these objectives is called Counterintelligence 21 or CI21. The initiative "would create a national counterintelligence executive with independent resources and staff to act as a focal point and conduit between policy makers, Congress, and private industry on the one hand, and the intelligence, law enforcement, and defense communities on the other" (Kitfield 2862). The approach also called for the appointment of a counterintelligence czar to coordinate increased information exchanges between the intelligence, defense, and law enforcement establishments. The motives behind the creation of CI21 are laudable, but it is utterly unrealistic to assume that the addition of another bureaucratic dimension will miraculously prevent security failures.

To prevent security failures and compromises of secure information as well as those who collect it and analyze it, the intelligence community must simply be more cognizant of its own distinct culture. The intelligence mission, the workforce that pursues its objectives, and the resources those employees must employ to support national security priorities necessitate and create an organizational culture unlike no other. Intelligence professionals may only reduce security failures by developing and implementing cultural artifacts that address the divide between organizational assumptions and individual values. Recent improvements in these areas have proven it is possible to balance these elements of the intelligence community's organizational culture, but continued vigilance is necessary if the intelligence community wishes to avoid security compromises such as those achieved by Jonathan Jay Pollard, Aldrich Hazen Ames, and Robert Philip Hanssen.

WORKS CITED

"Agencies of the USIC." 5 Mar 2002: N. pag. <http://www.cia.gov/ic/nav2.htm>.

Bass, Bernard M. and Ryterband, Edward C. Organizational Psychology. 2nd ed. Boston: Allyn and Bacon, 1979.

Blitzer, Wolf. Territory of Lies. New York: Harper & Row, 1989.

Callum, Robert. "The Case for Cultural Diversity in the Intelligence Community." International Journal of Intelligence and Counterintelligence 14 (2001): 25-48.

Corn, David. "The company they keep." Washington Monthly July-August 1994: 34–35.

Frieden, Terry. "Judge orders secrets protected in spy case." CNN Law Center. 6 March 2001. Cable News Network. 18 Feb. 2002 <http://www.cnn.com/2001/LAW/03/06/spy.protective.order/>.

Gentry, John A. "A Framework for Reform of the U.S. Intelligence Community" 6 June 1995. 8 Jan. 2002: N. pag. <http://www.fas.org/irp/gentry>.

"Hanssen pleads guilty to spying." The Holland Sentinel Online 7 July 2001. 18 February 2002 <http://www.hollandsentinel.com/stories/070701/new_0707010023.shtm>.

Hitz, Frederick P. "The Future of American Espionage." International Journal of Intelligence and Counterintelligence 13 (2000): 1-20.

Hulnick, Arthur S. "Intelligence and Law Enforcement: The 'Spies Are Not Cops' Problem." International Journal of Intelligence and Counterintelligence 10 (1997): 269-284.

Karnow, Stanley. Vietnam: A History. New York: Penguin, 1991.

Kitfield, James. "Anti-terror Alliance." The National Journal February 2001: 51+.

---. "Covert Counterattack." The National Journal 16 September 2000: 2858 - 72.

Klein, Rochelle. "Ethnic Versus Organizational Cultures: The Bureaucratic Alternative."" International Journal of Public Administration March 1996: 323 – 43.

Lowenthal, Mark M. Intelligence: From Secrets to Policy. Washington, D.C.: Congressional Quarterly, 2000.

Moynihan, Daniel P. "The Culture of Secrecy." The Public Interest 125 (1997): 55-78.

Pekel, Kent. "The Need for Improvement." Studies in Intelligence Spring 1998. 26 Jan. 2002 <http://www.odci.gov/csi/studies/spring98/index.htm>.

"Regulations blunted CIA effectiveness." BBC News n. d. 12 Feb. 2002 <http://news.bbc.co.uk/hi/english/audiovideo/programmes/panorama/newsid_1688000/1688524.stm>.

Riley, Patrick R. "CIA And Its Discontents." International Journal of Intelligence and Counterintelligence 11 (1998): 255-269.

Rosenbloom, David H. Public Administration. Ed. David H. Rosenbloom. 4th ed. New York: McGraw-Hill, 1998.

Schein, Edgar H. Organizational Culture and Leadership. San Francisco: Jossey-Bass, 1985.

---. Organizational Psychology. Ed. Richard S. Lazarus. 3rd ed. Englewood Cliffs: Prentice-Hall, 1980.

Shelby, Richard C. "Quotes about the Robert Hanssen Case, Part II." Online posting. CICentre. 28 May 2001 <http://cicentre.com/DOC_Quotes_Robert_Hanssen_Case_II.htm>.

Smith, Jeffrey H. Senate Judiciary Committee. Testimony. 25 April 2001. 10 Dec. 2001 <http://www.fas.org/sgp/congress/2001/042501_smith.html>.

Thomas, Stafford T. "The CIA's Bureaucratic Dimensions." International Journal of Intelligence and Counterintelligence 12 (1999): 399-411.

Turner, Michael A. "CIA-FBI Non-Cooperation: Cultural Trait or Bureaucratic Inertia?" International Journal of Intelligence and Counterintelligence 8 (1995): 259-273.

United States. Central Intelligence Agency. Joint CIA-FBI Press Release on Arrest of Harold James Nicholson 18 November 1996. 1 Feb. 2002 <http://www.cia.gov/cia/public_affairs/press_release/archives/1996/ pr111896.htm>.

---. ---.. Office of the Inspector General. Unclassified Abstract of the CIA Inspector General's Report on the Aldrich Ames Case. Washington: GPO, n.d.

---. ---. "Terrorism FAQs" n.d. 12 Feb. 2002 <http://www.cia.gov/terrorism/faqs.html>.

---. Executive Order 12333. 46 FR 59941, 3CFR. 1981.

---. Commission on the Roles and Responsibilities of the United States Intelligence Community. "The Central Intelligence Agency" 20 May 1996. 12 Dec. 2001 <http://www.access.gpo.gov/su_docs/dpos/epubs/int/pdf/int010.pdf>.

---. Dept. of Justice. "Hanssen Pleads Guilty to Espionage" 6 July 2001. 18 Feb. 2002 <http://www.usdoj.gov/opa/pr/2001/July/305civ.htm>.

---. ---. Federal Bureau of Investigation (FBI). Affidavit in Support of Criminal Complaint, Arrest Warrant and Search Warrants. Alexandria: United States District Court for the Eastern District of Virginia, 2001.

---. ---. ---. Statement of FBI Director Louis J. Freeh On the Arrest of FBI Special Agent Robert Philip Hanssen 20 February 2001. 1 January 2002 <http://www.fbi.gov/ pressrel/pressrel01/hanssen.htm>.

---. ---. Office of the Inspector General. A Review of the FBI's Performance in Uncovering the Espionage Activities of Aldrich Hazen Ames. Washington: GPO, 1997.

---. National Archives and Records Administration (NARA). "Records of the Central Intelligence Agency" 10 Dec. 2001. 5 Mar 2002 <http://www.nara.gov /guide/rg263.html>.

---. Senate. Judiciary Committee. "Jeffrey H. Smith Polygraph Testimony." 107th Cong., 1st sess. Washington: GPO, 2001.

---. ---. ---. Select Committee on Intelligence. An Assessment of the Aldrich H. Ames Espionage Case and Its Implications for U.S. Intelligence. 104th Cong., 1st sess. Washington: GPO, 1994.

---. The White House. Office of the Press Secretary. U.S. Counterintelligence Effectiveness 3 May 1994. 18 February 2002 <http://www.fas.org/irp/offdocs/pdd24.htm>.

50 USC Sec. 403-3. 2000.

Walsh, Lawrence M. "A Matter of Trust." Informatian Security April 2001. 12 Jan. 2002 <http://www.infosecuritymag.com/articles/april01/columns_note.shtml>.

Wettering, Frederick L. "Counterintelligence: The Broken Triad." International Journal of Intelligence and Counterintelligence 13 (2000): 265-294.

Woolsey, James. Interview. Capital Q&A. United Press International, 15 Mar. 2001.

VITA

Troy Michael Mouton was born in Lafayette, Louisiana, on October 7, 1970. He grew up in pastoral Cankton, Louisiana, and in 1988, he graduated from Sunset High School. Troy has one brother, Paul Bryan Mouton. His beloved parents are Paul Bennett and Venola Marie Seaux Mouton. Troy's military assignments and employment experiences piqued his interest in intelligence affairs and public administration. In May 1996, Troy graduated *Summa Cum Laude* with a Bachelor of Arts degree in English from the University of Southwestern Louisiana in Lafayette, Louisiana. He expects to receive his Master of Arts in Liberal Arts degree in May 2002. Troy resides in Baton Rouge, Louisiana, with his wife and best friend, Glenis K. Mouton.