**Procedural counter measures**

The physical protection of information, assets and personnel is fundamental to any security system. Closely related to physical security are the technical security safeguards required to protect certain facilities against intelligence collection or observation and security procedures adopted to monitor and control physical access to facilities and material. Government rules for protection of classified information cover construction and storage requirements (facilities, locks, alarms, guards), technical security requirements imposed on facilities storing classified information (surveillance countermeasures, TEMPEST, audio attenuation), and procedures affecting the conduct of operations within these facilities (inspections, document control, visit certification, and badges).

The Commission's focus was primarily on the domestic environment where there is the greatest potential for cost savings, a lower level of threat, and because it lends itself more readily to uniformity than do facilities at overseas locations. Our review was limited to the protection of classified information and material. It did not include protection of weapons, munitions, or nuclear devices which are governed by separate regulations.

Recently there have been significant policy changes affecting physical security within the Intelligence Community. However, it appears that cross-program management for physical, technical, and procedural security countermeasures is not uniform. The relationships with industrial contractors vary from punitive compliance inspections to problem-solving advice and assistance. In addition, many of our physical security policies are out of date, are not based on actual threat, conflict with each other, and have not been implemented in a uniform fashion. As a result, the end user is faced with a patchwork of multiple standards, increased costs because facilities cannot be shared, and irrational situations where information classified at a lower level (Confidential and Secret) is often more stringently protected than our government's most sensitive technologies and operations. The wide variety of physical, technical and procedural security requirements imposed on industry is the principal concern that lead to the development of the National Industrial Security Program (NISP).

*For Confidential and Secret information, the Defense Industrial Security Program requires that contractors be inspected every six months, that guards physically check safes that hold classified material, and that stringent document control audits and inventories be maintained. Director of Central Intelligence representatives normally inspect facilities housing Sensitive Compartmented Information once every two years, require alarms rather than expensive guards, and recently have dropped strict document handling requirements.*

The Commission seeks to apply physical, technical, and procedural security consistent with the same basic risk management principles recommended throughout this report. Security standards should provide two uniform degrees of protection for classified information. Decisions to adopt special protection safeguards should be based upon risk management analysis of the value of the asset, the threats and vulnerabilities, and the costs of protection. The relationship between government and industry should be a problem solving partnership that maximizes reciprocity. New procedural mechanisms should be instituted to terminate unnecessary controls and facilitate ease of reassigning cleared personnel.

**Physical Security Standards**

Today's physical security policies evolved in the context of the Cold War when it was often assumed the enemy would attempt penetration and it was necessary to keep them out at almost any cost. Organizations began to individually adopt different rules governing the protection of classified information. As a result there is no single facility standard. Facilities cleared for DoD Special Access Programs have rules which may vary from facility to facility and from program to program. Facilities housing Sensitive Compartmented Information (SCI) are governed by the Director of Central Intelligence Directives. Facilities holding collateral information follow differing standards depending on which organization is the sponsor. Application of these differing standards by individual government agencies is also uneven, resulting frequently in one government agency being unwilling to share space with another agency even though they both ostensibly use the same standard.

A facility's security may include alarms, guards, security containers (safes), access control devices, closed-circuit television, locks, special construction requirements, and a host of other countermeasures. It also may include a requirement for two people to be in close proximity at all times so as to deter the unauthorized removal or copying of classified material. With total risk avoidance as the goal, the addition of each of these countermeasure is justified by assuming that the countermeasure will provide an additional measure of protection. Cost is not a factor.

*The physical security countermeasures at one industrial facility include a fence, roving guards, and automated building access controls. Inside the facility, there is also a specially constructed room to which access is controlled by cipher and combination door locks. Moreover, the program manager of a special access program required that the five-drawer safe used to store program material have each drawer alarmed even though the safe was inside an area already alarmed.*

Yet the great majority of past compromises have involved insiders, cleared persons with authorized access who could circumvent physical security barriers, not outsiders breaking into secure areas. We have had numerous incidents of classified information being removed by cleared personnel, but no documented evidence leading us to believe an agent of a foreign power has ever broken into a classified area inside the United States.

In reviewing the existing standards for physical security and their implementation in practice, the Commission found that the amount of physical security provided to protect classified information in facilities within the United States is often excessive.

The Commission acknowledges the significant and ongoing policy changes affecting physical, technical, and procedural security requirements that are being developed, especially through the DCI Security Forum and the National Industrial Security Program task forces. Many improvements have already been introduced and some cost savings already realized. For example, the recent DCI policy decision to drop the two-person rule has permitted manpower savings in some contracts. Other elements, such as the military SAPs, continue to enforce this requirement. Not only do these inconsistencies produce confusion, they seriously erode the user's faith in legitimate security practices. Despite some positive efforts, the Commission concludes that many of the rules governing physical and technical protection of classified information stored within the United States have yet to realistically reflect the actual threat.

The Commission believes that an integrated systems approach based on valid risk management analysis must be implemented to replace the current fragmented process. Under risk management, each countermeasure can be viewed in the context of a fully integrated system. The introduction of two uniform degrees of physical security protection will remedy the current inconsistencies and permit the establishment of a more rational approach to the physical protection of information and material.

**Recommendation 43**

The Commission recommends that classified material or information stored within the United States be protected by one of two levels of a national physical security standard.

**Facility Certification**

Multiple standards, variously interpreted have inhibited, primarily in the DoD, the efficient sharing of facilities and services, resulting in increased cost to the US Government. Sharing is more prevalent in the Intelligence Community where areas used for storing and discussing Sensitive Compartmented Information (SCI) are built to standards contained in a DCI Directive. For years, these areas, called Sensitive Compartmented Information Facilities (SCIFs), have been certified by the first agency to use that particular space. Written agreements allow additional agencies to use the same facilities, accepting any waivers to the standards. Facility clearance reciprocity is less prevalent (but increasing) for Special Access Programs. All too often SAPs levy additional requirements by forcing contractors to add costly and excessive security upgrades or even build a new SCIF (or SARF-Special Access Required Facility).

*One west coast contractor said that the Intelligence Community usually grants approval for co-utilizing SCIFs within 48 to 72 hours. Yet the same process usually takes 4 to 6 months in the SAP world. Additionally, SAP program managers may levy further requirements, such as one manager who wanted $30,000 in upgrades made to an already accredited SCIF.*

The Commission supports co-utilization of certified facilities and further believes a registration system would help enforce this process. Once certified, a facility should be registered in a central data base. All government organizations desiring to operate at the relevant security level should accept the registered area without changes, enhancements, or upgrades. The facility should also remain certified until it is modified or closed out. Co-utilization of facilities is endorsed by the NISP and this registration process would complement the NISP effort.

**Recommendation 44**

The Commission recommends a data base registering certified facilities be established and that co-utilization and reciprocity of accredited space be mandatory.

**Facilities, Containers, and Locks**

While uniform standards are important, the standard itself must be supported by an analysis of actual threat and a reasonable risk management response. The importance of this is shown by the example of the national standard adopted for security containers and locks. Current national policy requires classified material be stored in GSA-approved safes or containers with approved locks. Exceptions to this policy were routinely made in domestic settings during the Cold War in acknowledgment that other layers of security were in place or because of site specific factors such as floor loading restrictions. Non-GSA-approved containers (bar lock cabinets equipped with changeable combination locks) and the open storage of classified information in specially constructed areas have been routinely allowed. There is no evidence that these waivers have compromised security. The risk management approach embodied in granting these waivers should become the basis for developing future policies. The Commission strongly opposes recent efforts that are calling for more stringent standards. An example is the current effort to replace existing container locks with the new GSA-approved electro-mechanical locks. This replacement effort is not based on current threat data and will significantly increase costs. For example, one west coast contractor estimates that replacing all the locks for its facility would cost more than $7.3 million. While new locks could be used in new containers, the Commission found no evidence that would warrant a large-scale replacement effort for locks already installed in approved facilities within the United States.

**Recommendation 45**

The Commission recommends that there be no replacement or retrofit of containers and locks currently approved for use in the United States.

**Industrial Security Inspections**

Companies with classified government contracts are periodically inspected to ensure they are protecting classified material in ways consistent with government security standards. These inspections take many forms to include an initial accreditation inspection, a change of status inspection when there is new ownership or new spaces, and special interest inspections based on a specific incident, investigative lead, or threat. In addition to these accreditation and incident-driven visits, there also are routine re-inspections required on a varying and arbitrary periodic basis depending on the contract and sponsor. These routine inspections are conducted by the DIS, the DoE, the CIA, the NSA, or any number of individual DoD SAPs, all using a variety of standards. The CIA and the DoE inspect every two years, allowing the contractor to self-inspect on the off years. Until recently, the NSA maintained a six month schedule. The DIS, responsible for the majority of the inspections, also reviews all aspects of a contractor's security program every six months. Less than one percent of these inspections result in unsatisfactory ratings. Both the frequency and value of these routine inspections were questioned by contractors interviewed by the Commission.

*One contractor stated that in 1992, DIS spent 480 hours inspecting the contractor's five facilities. But in 1993, despite the contractor's 38-percent reduction in personnel, 68-percent drop in documents, 40-percent less controlled area, and 50-percent fewer classified holdings, DIS needed 1413 hours to inspect the same five facilities.*

Contractors with Special Access Programs are inspected on a program-by-program basis with each individual project having its own requirements. For example, a contractor with six SAPs may undergo six separate inspections with each having differing requirements. Contractors state that routine re-inspections are time-consuming, onerous, costly, and confusing. They advise that the redundant inspections contribute little, if any, additional security.

*One contractor had to contend with 26 inspections by DIS and SAPs over a 10-month period in 1993. Inspectors were on-site for 99 out of 210 workdays. An additional week of planned inspection was canceled.*

Intelligence Community inspectors put less weight on fault finding and more emphasis on program review. For example, they may frequently visit a contractor to discuss programmatic or individual personnel security issues but rarely conduct formal top-to-bottom inspections. Some Intelligence Community components use award fee contracts with monetary awards as incentives for good security. The Commission endorses the partnership or service approach towards security, rather than an adversarial approach.

The Commission supports accreditation visits and special issue investigations, but sees no need for each organization to conduct routine inspections. These reinspections frequently involve a top-to-bottom review of construction, storage, and procedures complete with formal out-briefings to senior management. They also often require an official response from the senior management. Our vision of a government and contractor partnership rejects the concept of these punitive inspections. The Commission believes that multiple compliance inspections and re-inspections are costly, time consuming, and of questionable value in providing better security. A partnership or service-based approach should be encouraged.

**Recommendation 46**

The Commission recommends that, after an initial accreditation inspection, reinspections be limited to aperiodic, random inspections or those in reaction to specific incidents or threats. Routine industrial security re-inspections should be eliminated.

**TEMPEST**

TEMPEST (an acronym for Transient Electromagnetic Pulse Emanation Standard) is both a specification for equipment and a term used to describe the process for preventing compromising emanations. The fact that electronic equipment such as computers, printers, and electronic typewriters give off electromagnetic emanations has long been a concern of the US Government. An attacker using off-the-shelf equipment can monitor and retrieve classified or sensitive information as it is being processed without the user being aware that a loss is occurring. To counter this vulnerability, the US Government has long required that electronic equipment used for classified processing be shielded or designed to reduce or eliminate transient emanations. An alternative is to shield the area in which the information is processed so as to contain electromagnetic emanations or to specify control of certain distances or zones beyond which the emanations cannot be detected. The first solution is extremely expensive, with TEMPEST computers normally costing double the usual price. Protecting and shielding the area can also be expensive. While some agencies have applied TEMPEST standards rigorously, others have sought waivers or have used various levels of interpretation in applying the standard. In some cases, a redundant combination of two or three types of multilayered protection was installed with no thought given either to cost or actual threat.

*A general manager of a major aerospace company reports that, during building renovations, two SAPs required not only complete separation between their program areas but also TEMPEST protection. This pushed renovation costs from $1.5 million to $3 million just to ensure two US programs could not detect each other's TEMPEST emanations.*

In 1991, a CIA Inspector General report called for an Intelligence Community review of domestic TEMPEST requirements based on threat. The outcome suggested that hundreds of millions of dollars have been spent on protecting a vulnerability that had a very low probability of exploitation. This report galvanized the Intelligence Community to review and reduce domestic TEMPEST requirements.

Currently, many agencies are waiving TEMPEST countermeasures within the United States. The rationale is that a foreign government would not be likely to risk a TEMPEST collection operation in an environment not under their control. Moreover, such attacks require a high level of expertise, proximity to the target, and considerable collection time. Some agencies are using alternative technical countermeasures that are considerably less costly. Others continue to use TEMPEST domestically, believing that TEMPEST procedures discourage collection attempts. They also contend that technical advances will raise future vulnerabilities. The Commission recognizes the need for an active overseas TEMPEST program but believes the domestic threat is minimal.

Contractors and government security officials interviewed by the Commission commend the easing of TEMPEST standards within the last two years. However, even with the release of a new national TEMPEST policy, implementation procedures may continue to vary. The new policy requires each Certified TEMPEST Technical Authority (CTTA), keep a record of TEMPEST applications but sets no standard against which a facility can be measured. The Commission is concerned that this will lead to inconsistent applications and continued expense.

Given the absence of a domestic threat, any use of TEMPEST countermeasures within the US should require strong justification. Whenever TEMPEST is applied, it should be reported to the security executive committee who would be charged with producing an annual national report to highlight inconsistencies in implementation and identify actual TEMPEST costs.

Domestic implementation of strict TEMPEST countermeasures is a prime example of a security excess because costly countermeasures were implemented independent of documented threat or of a site's total security system. While it is prudent to continue spot checks and consider TEMPEST in the risk management review of any facility storing specially protected information, its implementation within the United States should not normally be required.

**Recommendation 47**

The Commission recommends that domestic TEMPEST countermeasures not be employed except in response to specific threat data and then only in cases authorized by the most senior department or agency head.

**Technical Surveillance Countermeasures (TSCM)**

Technical Surveillance Countermeasures (TSCM) involves the search for technical surveillance devices or "bugs." The TSCM function is decentralized within the government and resources and requirements are determined at the department or agency level. Traditionally, TSCM teams conduct inspections of domestic facilities when they first open and on a routine basis thereafter. TSCM teams are also called upon when there is some indication of a threat. A recent classified study shows that over the last 40 years, initial and routine domestic inspections uncovered few bugs, with the exception of an occasional hazard such as an on-line telephone connection or a two-way intercom into a secure area. The study also notes that few finds are uncovered in areas where good physical security and access controls are in place and that the overwhelming number of technical attacks against US interests occur overseas.

The failure to discover any use of technical surveillance devices domestically, coupled with budgetary pressures, influenced the application of TSCM. Within the last two years, the interagency TSCM training academy and two technical security laboratories have had to curtail their operations because of lost funding.

Although there is little or no evidence of a domestic threat, the Commission believes that overseas locations can be very vulnerable to technical invasion. It is therefore very important to maintain an active, focused, interagency R&D program in support of TSCM. Scarce resources should be directed both to specific threat-driven inspections and to the maintenance of an R&D and training effort.

**Recommendation 48**

The Commission recommends:

a) The elimination of routine TSCM inspections within the United States in favor of increased emphasis on overseas inspections. Any domestic TSCM efforts should be specifically threat driven.

b) The government fund a coordinated TSCM R&D and training program to support overseas inspections and as a defense against future technological advances in technical surveillance equipment.

**PROCEDURAL SECURITY**

**Central Clearance Verification**

The verification of an individual's clearance and level of access is a critical component in the management of interagency and industry visits to classified areas. On any given day, thousands of clearance access requests are made. Hundreds of personnel are officially involved in clearance verification. Many more are involved peripherally, and failure of the process affects most cleared persons at some point.

The typical visit request goes through at least six steps, involves at least three levels of the bureaucracy at each agency, and can take anywhere from one to three days. One security manager stated that she spends some 40 percent of her time handling visit requests, and, that she must rely on personal contacts and informal channels to get the job done. Considering the hundreds of visits conducted daily within the community, the productivity loss is enormous. All too often, individuals ask their security officer to pass clearance information, and, when they arrive at a meeting location, they are told, "We did not receive your clearance, you cannot enter the building." A flurry of calls between the visitor and his security officer determines that the clearances were sent, despite the fact that the receiving office has no record of the incoming clearance. Time elapses, sometimes after heated exchanges, the clearance information is orally passed, and the meeting starts:

*Despite having his clearance passed a week before a quarterly meeting at the CIA, a senior military officer was delayed some 30 minutes while his military assistant, whose certification was passed and received at the same time, had no difficulty entering.*

The current clearance verification system draws upon clearance information contained in data bases maintained by the OPM, the DoD, and the CIA. Some highly sensitive programs, for example, the DoD SAP community, also maintain clearance/access data bases that are withheld from the major data bases. The CIA community-wide data base for certifying access to Sensitive Compartmented Information (SCI) is obsolete and scheduled to be replaced within two years. The DoD's Defense Clearance Investigative Index (DCII) is being upgraded and will be interconnected with the Federal employment Suitability and Security Investigations Index (SSII) maintained by OPM. The DoD and the OPM data bases contain more than 95 percent of all collateral clearances. The proposed CIA system will include all of the SCI clearances. By combining these data bases and adding special programs, the user community would have a Central Clearance Verification System (CCVS). Such a system would reduce duplicative record systems, administrative processing, time delays, and personnel requirements. In addition, a central clearance data base would provide the information backbone for the application of "smart-card" technology for instant clearance verification (without human intervention) for access to networks, E-mail, and facilities.

**Recommendation 49**

The Commission recommends that a Central Clearance Verification data base be developed and made available to industry and government. The data base should contain all collateral and SCI clearances. Sensitive clearance information should be encrypted or otherwise protected within the data base.

**Certification of Contractor Visits**

The DoD industrial security rules require stringent control and prior approval of contractor visits, especially when classified information is to be discussed. Contractor visit requests must be provided, in writing, in advance of an actual visit. However, under certain circumstances, contractor visit requests must also contain a signed certification from the cognizant government contracting officer or prime contractor that the visitor has a need-to-know under a particular contract for access to classified information. This policy does not apply to government employees.

The requirement to certify need-to-know for each individual visit request between contractors without a direct classified contractual relationship, has increasingly caused significant problems and needless delays. Contractors question the need for the certification process in view of the heavy dependence of the process on paper. They maintain that the advent of facsimile machines and data base management systems for transmitting visit requests renders the exercise of obtaining a contracting officer's signature on each paper visit request obsolete. Critics also cite the practical difficulty in locating a government authority to certify individual visits. In many cases, government certification of need-to-know is in fact a rubber stamp. In circumstances such as contractor attendance at classified symposia and conferences involving general technical areas or subjects unrelated to any particular classified contract, the certification rule becomes a real impediment to accomplishing normal, legitimate business.

The Commission believes that the requirement for need to know certifications for contractor visits involving generally protected projects is outdated, imposes a dual standard for government and industry security, and should be abolished. The process unnecessarily complicates and slows the accomplishment of necessary business and inhibits the exchange of information that should take place between properly cleared and accessed personnel. A requirement for government certification of a contractor's need to know should be restricted to those contractor visits or meetings involving specially protected projects, rather than a blanket requirement for all classified visits between contractors without a contractual relationship.

**Recommendation 50**

The Commission recommends that the requirement for government certification of need-to-know for contractor visits at the generally protected level be abolished.

**Communitywide Badge Systems**

Interagency access procedures established by various security organizations serve two basic functions: to verify a person's identity and to validate clearance level. Virtually all agencies controlling access to their facilities rely on badges (permanent staff and visitor), automated and/or guard access controls, and administrative procedures for certifying and transferring clearance information. Over the years, each agency has developed its own badging system, visitor control process, and escort requirement to restrict unauthorized access. When outsiders seek access on official business, however, the system frequently breaks down. Badges are unique to each agency and vary in sophistication, that is, from serving purely as visual recognition to offering considerable encoded information readable by automated equipment at the point of entry. Thus, the lack of standardization makes for cumbersome procedures and contributes to frequent visitor delay at entry points. In many instances, cleared personnel must complete the same forms, sign the same waivers, and adhere to the same escort requirements as uncleared visitors, despite having had their clearances passed. One security manager stated, "The visit processing procedure is a cottage industry in need of modernization."

Several intelligence agencies (the CIA, the NSA, and the DIA) have recently adopted limited badge reciprocity in an effort to streamline interagency visit procedures. Critics of the reciprocity program contend that it is difficult to administer (too many badges for guards to remember, reader incompatibility, and so forth), and that variability in implementing reciprocity has exacerbated an already inefficient process. For example, a CIA employee on an official visit to the NSA under the new badge reciprocity procedure must still visit the NSA central badge office, fill out and sign a form, get an NSA visitor badge, and wait to be announced to his or her host by the receptionist, exactly the same steps as would have to be performed if the visitor had no badge at all.

The Commission concludes that the current badge control procedures are costly and impede interagency business by authorized personnel. The Commission is aware that the DCI Security Forum has tasked the NSA with development of a community badge and that similar efforts are under way within the DoD and the DoE. These efforts should be coordinated and combined to provide a single-badge standard throughout the security community.

**Recommendation 51**

The Commission recommends the development of a uniform badge system for the government's cleared community. The badge system should provide for visual and electronic recognition, automated access control, and encoded level of access.

**Document Tracking and Control**

The DoD Industrial Security Manual (ISM) requires itemized accounting and verification of Secret documents held by industry in support of classified contracts. The DoD does not apply this standard internally. Neither the DoE nor the CIA have this requirement for their contractors, and the Director of Central Intelligence just approved the NRO's request for elimination of this requirement for certain Secret SCI documents. Moreover, the Task Force on Classification Standards recommended that accounting or strict tracking requirements for Top Secret material in SCI facilities be eliminated.

Contractors contend that document tracking and inventory requirements do not enhance security and are very costly. One major contractor estimates a single classified document requires 98 minutes handling time annually. Results from an informal survey conducted by the Commission suggest that eliminating the requirement to precisely track every Secret document could reduce document control personnel staffs by some 40 percent. Most contractors would continue to maintain a basic data library function, but security requirements for extensive inventories and recording of internal transfers would be eliminated.

A number of senior government officials similarly have questioned the cost effectiveness of this type of document accountability. Some have opined that it is an expensive control system but that they know of no case in which document accountability has led to the identification of a spy. We have heard that when accountable documents are missing, time-consuming inquiries inevitably led to the conclusion that the material was "inadvertently destroyed." One senior official has stated that the elimination of document tracking would not degrade security but could result in substantial savings if manpower associated with the current process is eliminated.

Contractors also object to the need for extensive justification and protracted negotiations currently required for retention of classified documents when a contract is completed. They must frequently "reinvent the wheel" because information generated for one contract cannot be used in performance of another. Required to turn information in at the completion of a contract, a contractor must then approach the government and ask for the product that was originally generated by the contractor. Contractors also note that the regulations are inconsistent, providing for retention of R&D classified information but not routine contract materials.

The Commission believes that the integrity and trustworthiness of personnel is the key to the proper protection of documents. Strict document accounting and retention practices are costly and do not deter compromise of information. To those who would cause damage, personal computers, facsimile machines, copier equipment, and modems and networks, available in the normal office environment, offer opportunities to compromise documents without detection despite elaborate and costly physical document accountability and control procedures.

The procedures mandated by the DoD Industrial Security Manual to account and track documents do not provide real protection. There is no value in accounting for the physical possession of 100 documents in the morning and 100 at the end of the day if at midday they can be copied electronically without detection and transmitted to an unauthorized party. There is no evidence that the lack of tracking of Secret documents in government offices has led to an increase in compromises. The industrial standard should be no different.

**Recommendation 52**

The Commission recommends that:

a) The requirement for internal tracking and inventory and periodic inspections of classified documents be eliminated.

b) Contracts be amended to allow routine retention of classified documents provided that they are properly safeguarded.

**Document Destruction**

There are also similar accounting and verification requirements for the destruction of classified documents. DoD internal regulations generally require records of destruction and the imposition of the two-person rule for Top Secret documents destroyed by government employees. There is a two-person rule but no destruction record required for Secret documents, and only one cleared person is required to destroy Confidential documents.

The DoD Industrial Security Manual requires destruction records and the two-person rule for destruction of both Top Secret and Secret documents; only one person is required to destroy Confidential documents. The DoE does not require records of destruction for either Secret or Confidential.

For SCI documents there generally is no requirement for destruction certification, but there is a two-person rule.

The same logic that compels us to recommend the elimination of document accountability drives the conclusion that document destruction accountability requirements are a cost without a significant benefit, and the requirement should be eliminated. Anyone who wants to remove classified information can do so while leaving the accountable record copy untouched and then properly accounting for its destruction. Destruction records, which must be duly dated, signed, and retained, and the two-person rule represent avoidable costs that give no more than an illusion of security.

**Recommendation 53**

The Commission recommends that item-by-item document destruction accountability be eliminated.

**Document Transmittal**

In the current environment, encrypted data transmission should be the rule. Expensive, labor and time intensive document transmittal by mail service or courier should be the exception.

To the extent that it is necessary to utilize older methods of document transmittal, we recommend a standard be adopted for generally protected information and one for specially protected information.

Currently, DoD internal regulations allow Confidential documents to be transmitted in US postal channels either by first class mail or by certified mail; Secret documents must be sent by registered mail; Top Secret, SCI and SAP documents must either be sent by courier or hand-carried by appropriately cleared and authorized persons. The Industrial Security Manual requires use of US postal service express or registered mail for Secret and certified mail for Confidential documents.

The Commission believes there are no significant risks in routinely using registered or certified mail for transmitting generally protected information. In some cases, first class mail or commercial services are adequate.

The Commission also believes that the expense of using couriers or hand carrying all specially protected information is unwarranted in most cases. Registered mail is used to safely transport expensive jewels and high-value negotiable instruments. At the specially protected level, managers should also have the option of using certified or registered mail instead of being forced to use expensive couriers. While the Commission believes transmission options should be expanded, the decision on which mode is best suited for individual programs should be made at the local level.

**Recommendation 54**

The Commission recommends that the document transmittal rules be revised for both generally protected and specially protected information. Generally protected documents should be sent by US first class, certified, or registered mail, or by a commercial delivery service. Specially protected documents should be sent by either US registered mail or by courier.

**Operations Security**

Some elements of the intelligence and defense community have been using the risk management process for many years under the rubric of Operations Security (OPSEC). Growing out of lessons learned in the Vietnam war, OPSEC seeks to "control information and observable actions about one's capabilities, limitations, and intentions so as to prevent or control their exploitation by an adversary.S (Footnote 18) Emphasis is placed on the analysis of unclassified information and public sources.

Seeking to institutionalize this process, in 1988 National Security Decision Directive (NSDD) 298 mandated the implementation of a formal OPSEC program by each executive department and agency with national security responsibilities. It designated the Director of NSA as executive agent for OPSEC programs and tasked him to establish and maintain an Interagency OPSEC Support Staff (IOSS)19 to provide consultancy and training for executive departments and agencies required to have formal OPSEC programs.

The Commission believes that there is a clear and compelling need for operational security in a military environment and in the conduct of sensitive operations. However, in the years since the establishment of the National Operations Security Program, a formal OPSEC structure has developed apace, with OPSEC responsibilities being assigned at each organizational level of DoD service departments and agencies, at the DoE, and at other government departments and agencies. There is now a robust OPSEC community coexisting with, but for the most part, separate from the standard security structure. The OPSEC Professionals Society boasts of a membership of some 475 professionals, with membership being equally divided between government and the private sector.

OPSEC is perceived by many, particularly in industry, as just a new way to repackage security requirements using elaborate procedures. It is seen as a separate discipline not integrated with other security disciplines and competing with them for scarce resources. National OPSEC requirements are framed in such general terms as to provide insufficient guidance for program managers and resource allocation. Moreover, despite the NSA's training of over 2,200 individuals in the OPSEC process over the past 3 years, industry sources advise that government security managers, contracting officers, and program managers are not trained in and do not understand OPSEC methodology, rarely request OPSEC surveys, do not provide specific threat data, or inspect for OPSEC compliance. (Footnote 20) To meet the demands of government contracts, industry, which also has a shortage of experienced OPSEC people, must recruit and train people to provide consultant support to ongoing classified industrial programs at unwarranted expense.

No one interviewed by the Commission questioned the appropriateness of selecting cost effective security countermeasures based on the assessment of risk. What is questioned is the wholesale imposition of the separate OPSEC structure to all sensitive governmental activities, including classified contracts with industry. OPSEC should not be a separate program, but part of the risk management philosophy that is integrated throughout the existing security structure.

**Recommendation 55**

The Commission recommends that:

a) Executive departments and agencies integrate OPSEC principles into the normal security staff structure and that risk management processes be incorporated into security and security awareness training programs at all levels.

b) Mandatory requirements for formal OPSEC programs be deleted from all contracts except those in response to specific threats and then only when specifically authorized by the most senior department or agency head.

c) NSDD 298 be reviewed, revised, or rescinded in accordance with these new requirements for OPSEC.