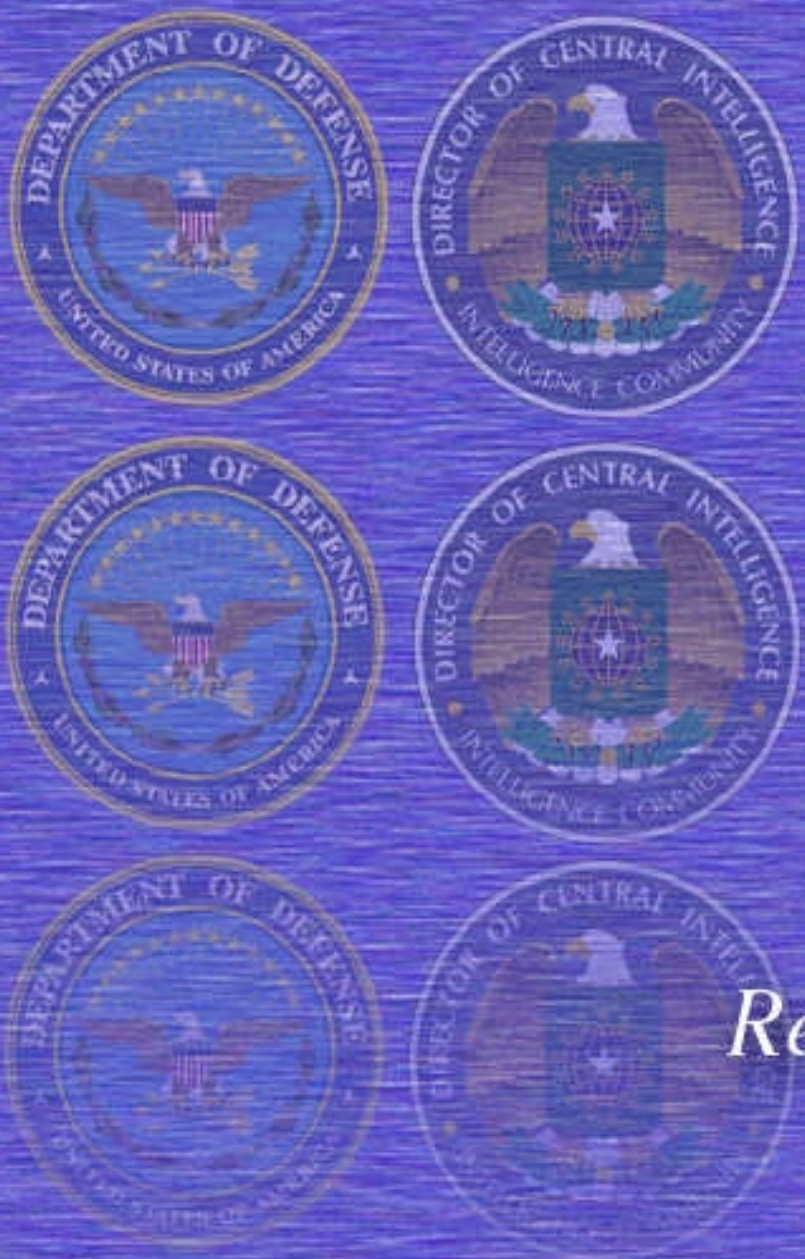

Report by the

JOINT SECURITY COMMISSION II

24 August 1999

Report of the Joint Security Commission II

August 24, 1999

TABLE OF CONTENTS

INTRODUCTION

Almost six years ago, the Secretary of Defense and the Director of Central Intelligence established the first Joint Security Commission, based on their belief that the Nation's security systems were slow to move beyond the Cold War, were inefficient, had built-in inequities, and cost more than they should. In February 1994, the Commission proposed a set of policies, practices, and procedures for a forward-looking, rational, fair, and cost-efficient security system. The Commission proposed the creation of the Security Policy Board to oversee development and implementation of security policy. The current Deputy Secretary of Defense and Director of Central Intelligence directed that the Joint Security Commission reconvene for two purposes:

- To assess progress toward the goals recommended in the original report of the Joint Security Commission and directed in PDD-29, as well as the continued relevance of those goals.
- To examine emerging security issues that may require increased emphasis as the security environment becomes increasingly dominated by electronic data systems, networks, and communications systems, and as business and technology become increasingly global.

Our report treats these two purposes in turn. Part I assesses the current state of progress towards the goals directed in PDD-29. Part II focuses on the increasingly vital business of the security of electronic information and information systems. We found a massive amount of effort underway in Information Systems Security (INFOSEC). We also found that the effort is in need of a clear enunciation of principles, goals, and definition of authorities and responsibilities. Two underrepresented but vital attributes of interconnected networks are the ability to provide essential services when under attack or when experiencing product or system failures, and having design features that provide for rapid recovery and restoration of full services after suffering a loss of capability.

INFOSEC is highly fluid and poses unique challenges, but requires security disciplines much like those that have long characterized good security practice. Personnel Security practice is intended to establish and maintain a reasonable threshold for trustworthiness through investigation and adjudication as a prerequisite to granting and maintaining access to classified information. At the same time, there is clear recognition that, because people change, the investigation and adjudication process can only assess identifiable past behavior and cannot ensure that only trustworthy people gain access or that trustworthy people will remain trustworthy. Hence, there is a need for various forms of monitoring within the system. Facilities Security establishes workspaces that are isolated from potential threats to some reasonable level, but security practices must also, through various forms of monitoring, protect against subsequent penetrations. Similarly, the first level of defense for INFOSEC is to create access controls to minimize unauthorized access to information and information systems. But, as in the case of Personnel Security and Facilities Security, access control cannot ensure that only authorized and trustworthy people gain access. Hence, security also demands capabilities to monitor activity within controlled access systems. It also demands quality people, and here INFOSEC presents one of its biggest challenges, for a pressing need exists to create a cadre of highly technical network security specialists who can continue to meet the security challenges created by the increasing reliance on information systems.

PART I: MEETING THE GOALS OF PDD-29

Progress in Policy and Implementation

The Security Policy Board structure has helped achieve significant progress in accomplishing the objectives described in PDD-29. The following sections discuss important issues where there have been varying degrees of progress. The sections cover important and difficult issues where:

- New policies have been developed, promulgated, and implemented through much of the Government;
- There has been important progress in developing policies but where work remains to promulgate new policies; and
- There has been much attention but only limited progress towards agreement on policies.

Areas Where New Policies Are Developed, Promulgated, and Partially Implemented

Developed and approved within the Security Policy Board process, approved by the President, and promulgated by the NSC, uniform adjudicative guidelines and investigative standards form the basis for reciprocity of both investigations and adjudicative decisions for classified access across the Government. With these standards and guidelines in place, there is no longer a legitimate reason to reinvestigate or readjudicate when a person moves from one agency's security purview to another. This policy saves time and resources and helps ensure fair and equitable treatment. These guidelines reflect hard-won compromises, incorporating tradeoffs between ideal security and the fiscal facts of life. Of particular importance is their recognition that, with extensive decompartmentation of once highly classified information, and with more and more sensitive material now available at the SECRET level, the SECRET-cleared population requires greater security attention than before. The regime they impose for SECRET access derives from this recognition. Still, there are important issues regarding the appropriateness of some of the standards that will need to be resolved. There are also important issues regarding the adequacy of any concept that focuses exclusively on protecting classified information. In the modern operational environment, it may be impractical or impossible to bring information critical to the mission under the safeguards provided by classification. These issues are discussed further in the "Key Underpinnings" section in this report.

There are other noteworthy accomplishments. The facilities security community, for example, working within the framework provided by the Board, has effectively achieved facilities reciprocity by issuing common standards that address relevant issues.

Areas of Progress in Developing Policies

The special access community, long regarded as a repository of arbitrary security practices, has made substantial progress toward more effective security by eliminating duplication and other venerable but questionable customs, by working toward much greater reciprocity of access eligibility decisions, and by standardizing security requirements across programs to a considerable extent. DoD's *Overprint to the National Industrial Security Program Operating Manual Supplement* has replaced multiple service-specific Special Access Program security manuals with a single set of rules; this is particularly valuable in industry, where

facilities housing multiple programs need no longer work to multiple sets of overlapping yet conflicting guidance.

The Security Policy Board forwarded the Safeguarding Directive required by EO 12958 to the National Security Council in December 1997; approval did not come until August 1999, more than a year and a half later. Yet the Safeguarding Directive is a key element of the national security program, updating uniform procedures for the handling, storage, transmission and destruction of classified information as a result of the replacement of EO 12356 by EO 12958, and establishing baseline definitions for designation of Special Access Programs (SAPs). In early 1998, the Forum approved and forwarded to the Board the financial consent form required by EO 12968; final Board approval came only a year later, and NSC action is still pending. These two examples suggest that closure is an issue that the Board must more aggressively address.

Areas of Limited Progress

The Board has not succeeded in addressing information systems security (INFOSEC), having been unable to create the intended INFOSEC committee, nor has it established a mechanism for oversight as PDD-29 provides. We discuss information systems security in Part II of this Report.

Future Challenges

Meanwhile, the security environment continues to be dynamic. Since 1994, the traditional boundaries of what we have regarded as security business have expanded to account for relevant changes in the security environment. Industry is increasingly global, and so are military activities as coalition operations are now the norm. The Internet has established rapid, worldwide connectivity, which means not only that Americans, including those in the most sensitive positions, have access to the world, but that the world has access to them. The era when the Government built its secure systems to its own specifications for its own people has given way to one in which outsourcing and use of commercial-off-the-shelf systems have become the business strategy of choice. These and similar changes offer new security challenges.

Key Underpinnings of an Effective Security System

Whatever the specific problem being considered—physical security, the classical task of protecting classified information, protecting computer and network systems, or protecting all classes of critical mission information—there are two basic underpinnings of an effective security system:

- Reliable and trustworthy people, and
- Training, education, security awareness, monitoring, and accountability of people and activities within the cleared system.

The following sections address these.

Reliable and Trustworthy People

Ensuring that all our people with access to classified information, to other mission critical information, and to information systems control and administration are and will remain reliable and trustworthy remains beyond the range of reasonable expectation. The achievable goal is for a system that maintains a reasonable and affordable standard for vetting people for reliability and trustworthiness. There has been continuing discussion about the rigor of the entry-level clearance process, with some citing the fact that the spies who damaged U.S. security interests were people who had such clearances. The Commission found that to be a circular argument; since we define spies as people who violate their trust by divulging classified information to unauthorized people, the spies under discussion will come from the population of cleared individuals.

Investigation and reinvestigation cannot carry the full burden of ensuring reliability and trustworthiness. Instead, the initial investigation provides assurance that a person has not already demonstrated behavior that could cause a security concern; it is predictive to the extent that past and future behaviors are related and to the extent that investigative practices are able to uncover relevant past behavior. Reinvestigation is an important, formal check to help uncover changes in behavior that have occurred after the initial clearance. It is, to some extent, analogous to a periodic physical. But just as a physical is only a part of a good health program, reinvestigation is only a part of continuing personnel security. Neither investigation nor reinvestigation relieves supervisors and seniors of the responsibility and accountability for being attuned to the continued security health of their people, and for identifying problems and working to solve them outside the routine reinvestigation cycle.

Some have suggested that the investigation standards should be tied to the individual's current access level. While that is, to some extent, a current practice, attempting to formally adjust the level of interest in the reliability and trustworthiness of individuals to their current level of access would, at best, be administratively very difficult. At worst, it would signal giving up on the idea of a standard that establishes confidence in all but a dangerous few who will dishonor their commitment to protect security information.

Controversy should not be about the importance of the goal, but about the utility of approaches to checking for reliability and trustworthiness. For example, there are three issues regarding background checks that continue to generate debate, each of which impacts cost and risk assessments. The three areas are neighborhood checks, telephone interviews, and financial data reporting. At present there is little analytical basis for judging the cost effectiveness of these measures. However, many security professionals strongly support them. Without analytical data on risk, there is little choice but to stay with long-standing practices in spite of doubts in parts of the community about their utility.

There are other important unknowns that need to be resolved to ensure that the process is expending resources on valid approaches to assessing reliability and trustworthiness. Data mining to detect anomalies that could indicate someone thought to be reliable and trustworthy is engaging in unauthorized activity is one example of a technique that may hold promise for reducing the amount of fieldwork. However, it could also have the opposite effect of generating leads that warrant further investigation. To make intelligent decisions about the future substance of personnel security, there is a critical need for authoritative research to determine the value of various practices.

The type of research envisioned is an interagency, multi-year effort, separately funded, conducted by research professionals under the direction of the Security Policy Board. The Commission notes efforts already underway, including the ongoing work to consolidate and coordinate personnel security research under Board auspices, recent funding initiatives in the Defense and Intelligence Communities, and a test of the cost and value of financial disclosure.

Modest resources are needed to conduct this needed research to determine whether extant security policies, standards, and criteria are adequate to support the operational security and mission assurance needs of departments and agencies in a threat-based and cost-effective manner. To help avoid duplication and waste, the commission suggests a discretionary budget line for the SPB to be used as bridge and seed money to fund projects executed by a designated department or agency.

Recommendation #1: The Co-Chairs of the Security Policy Board, leveraging efforts already contemplated or underway, should commission and fund a research effort to determine the efficacy of personnel security policies and to resolve issues about their effectiveness. The Co-Chairs should monitor this effort, ensure the proper assessment of its results, and use those results to develop appropriate policies.

The Security Research Center (SRC), formerly PERSEREC, no longer reports directly to OASD C^3I, but to the Defense Security Service (DSS). Because personnel security research must involve the whole process, not investigations alone, the SRC needs to report, not to the investigative agency, but to the policy element, which is OASD C^3I. Evaluating the results of research through the Security Policy Board structure can be expected to lead to new policies, and to their implementation. However, except in extraordinary circumstances where the benefits to be gained are immediate and substantial, the temptation for individual agencies to depart from agreed-to standards is detrimental both to standards and to interagency reciprocity. Likewise, the DoD Polygraph Institute (DoDPI) now reports to DSS. DoDPI must function as the Government's single polygraph institute, yet its organizational placement and even its name weigh against this. Like SRC, DoDPI should report to OASD C^3I; its name should be changed to the National Polygraph Institute to reflect more accurately its actual function.

Recommendation #2: DoD should reassign SRC to OASD C^3I; moreover, DoDPI should be redesignated the National Polygraph Institute with the Security Policy Board designated the National Manager and DoD OASD/C^3I the Executive Agent.

All Government agencies have agreed to background investigation and adjudication standards. The standard for reinvestigation is 5 years for TOP SECRET and 10 years for SECRET clearances. Failure to adhere to these standards can jeopardize reciprocity—acceptance of one agency's clearances by another. More important, such a failure signals to the workforce that the leadership does not believe in the security standards. Such an attitude could be highly detrimental to security awareness, monitoring, and accountability.

Further, many security professionals and the Commission believe that reinvestigations are even more important to ensuring reliable and trustworthy people than the initial clearance

investigation, since people who have held clearances longer are more likely to be working with more critical information and systems. Yet there are as many as 700,000 people listed in Department of Defense records as being overdue periodic reinvestigations, and the backlog still growing at the time of this report. CIA is also not meeting the standard for TOP SECRET clearances, but has developed a plan to reach the standard by 2000.

While 5 years and 10 years are arbitrary, the need for a standard that all agencies adhere to is not. Still, it is not feasible for the DoD to quickly dig its way out of the current situation regarding reinvestigations. Even if funding were no issue, it would take several years to provide the needed added investigators and to work through the backlog. Hence, the Commission suggests that DoD set near-term dates to start adhering to the standard as new reinvestigations come due. Further, the Department should screen all those overdue for reinvestigation to determine those who pose the greatest risk based on position and access, working off all those in that category as soon as possible. The Commission thus recognizes two priorities: first, to ensure that the vetting process is on track for all new entries, and, second, to ensure that a rational, risk-management approach is applied to reducing and ultimately eliminating the backlog. It is unlikely that DSS will have the capability to deal with this requirement. Hence, increased outsourcing may be needed. Regardless, the commitment of senior leadership and appropriate resourcing can solve this problem, as the example of the National Reconnaissance Office—which actually exceeds reinvestigation standards—proves.

At present, there is no limit on the duration of an interim clearance. DoD should set a limit of 180 days, requiring that the needed background checks and adjudication processes are completed within that period.

Recommendations #3 and 4:

- ***The Department of Defense should begin first to fully enforce the standards for reinvestigations and then, within 90 days, should screen all overdue for reinvestigation to identify those whose positions and access suggest the highest risk, and should provide the resources to complete those reinvestigations promptly; the Central Intelligence Agency should expeditiously execute its plan to eliminate its backlog by 2000.***
- ***DoD and CIA should set a limit of 180 days for new interim clearances, requiring that the needed background checks and adjudication process be completed within that period. In addition, they should screen all existing Interim clearances and promptly close out those where positions and access suggest the highest risk.***

For a number of years following the completion of the work of the Joint Security Commission in 1994, we saw little progress in addressing common standards for Special Access Programs (SAPs). In the past eighteen months, however, there has been an energetic and effective effort to apply the principles from PDD-29 to these programs. The engine for this progress has been the SPB-sponsored Special Access Program Security Standards Working Group (SAPSSWG).

While recent progress is encouraging, a continued focus will be required to complete this work. Significant issues remain, including full implementation of SAPSSWG-approved

personnel security reciprocity policies for SAPs and the elusive but desirable goal of reciprocity between the SAP and SCI communities. Fielding a SAP access database is essential to both efforts. Such a database, subject to appropriate security controls, would provide the single source for information regarding SAP eligibility determinations necessary for effective reciprocity. Its continued lack has stymied implementation of the genuine advances made in SAP policy.

Recommendations #5 and 6:

- ***The Security Policy Board should maintain a high priority on applying common standards to Special Access Programs and require that any needed policy recommendations go from the SPB to the NSC within 180 days.***
- ***DoD should immediately provide adequate funding and field a SAP access database, with appropriate security controls, to facilitate effective reciprocity.***

Reliability and trustworthiness are not requirements solely for those needing access to classified information, but apply as well to those in positions that are sensitive for reasons other than classified access. The question arises whether compartmenting security and employment suitability continues to make sense, or whether new policy should require a single program that assesses reliability and trustworthiness for both. Separate, though overlapping, Executive Orders—10450 and 12968—currently apply. There is a need to reexamine screening of personnel, both federal employees and contractors, whether for appointment to the federal, military, or foreign services, or for access to classified information or other sensitive information or facilities. Such a reexamination would recognize that harm to the nation can come from not only the improper actions of people who have access to classified information, but also from those of people with access to unclassified yet sensitive information, to computer systems, and to the critical infrastructures upon which our society depends.

Recommendation #7: The Board should propose to the NSC a new Executive Order that takes a comprehensive approach to addressing the suitability, reliability, and trustworthiness of persons employed in sensitive duties on work for the Federal Government. This would include individuals working in any capacity, and based upon the sensitivity of the duties, regardless of access to classified information. A proposal from the Security Policy Board for such an order is consistent with its stated mission in PDD-29.

Personnel security policies and practices must account for the fallibility of people and the inability to predict future behavior. Past behavior and present conditions, can *shape* what a person will do in the future but do not always *determine* it. Good personnel security, therefore, goes beyond the finding and sorting out of facts—the essence of investigation and adjudication—and moves toward creating a security-aware environment. In such an environment senior officials demonstrate a commitment to security; and from this flows the accountability of line managers. It enhances both security protections and security awareness by appropriate supplemental means; for example, some agencies may consider more frequent

counterintelligence polygraph examinations for people in particularly sensitive positions. Such an environment increases integrity by eliminating pointless opportunities to violate it. For example, it establishes straightforward, system-administered need-to-know regimes for classified material stored in electronic systems and eliminates unnecessary use of portable media. Clearly, ensuring the reliability and trustworthiness of the cleared workforce requires more than investigation, no matter how critical an element investigation is. It requires vigilance, awareness of people and their problems, and application of necessary if sometimes restrictive and intrusive security measures in a way that makes clear they exist to benefit those who must comply with them rather than to suggest that everyone is a suspect in some as yet undefined crime.

Education, Training and Awareness, and Accountability

The time from the Commission's last report to the present has been turbulent for the security-training field. Organizational downsizing and the reallocation of funding have adversely affected virtually every agency in the Executive Branch. Disbanding the Department of Defense Security Institute, which provided quality training for both DoD and non-DoD security professionals, has proven particularly damaging. Agencies that had depended on others for training have not only found their training budgets dramatically reduced, but have been challenged to find other Government courses able to accept external students, even with the remaining funds for training. Yet effective security awareness programs are essential for maintaining a workforce that is sensitive to security issues and that understands the relationship between security and the success of their own work. GSA, OPM, CIA, and DoD need to take immediate steps to re-vitalize their security training apparatus. Furthermore, because the need for training and awareness resources is significant, and because critical requirements can materialize outside the normal budgeting cycle's ability to react, a need exists for a ready source of bridge and seed money to initiate projects that a designated department or agency would then execute. Such monies could be best provided through a discretionary budget line through the SPB.

Security awareness is the responsibility of each supervisor and each individual with access to classified information or other mission critical information or systems. There is no substitute for a high level of such awareness at all levels and for accountability in line management. Counterintelligence and line management responsibility for security must go hand-in-hand: there can be no effective counterintelligence if left to a few professionals without the commitment of line managers who deal with their people every day.

Even so, a professional security force will continue to be essential to an effective program of security education, training, and awareness. It is important that this profession be considered a key part of the management and operational chain. Security, especially information systems security, has become an integral aspect of the national critical infrastructure. A robust national security training program is an important element of risk management. No one agency should bear the burden of supporting all of the Federal Government, but one or more agencies can lead with resources and attention to ensure that adequate security training will be available. The Department of Energy's Nonproliferation and National Security Institute provides one example of a coherent approach to security training that might serve either as a basis of or a model for a federal security training center. Future success in developing a national training program depends on obtaining adequate funding and support from the federal community. The

Commission supports continued efforts toward creating a national training program for security professionals.

Yet the role of the security professional is to lead and advise the process. Security is a line management responsibility. Effective security demands a cleared workforce that is knowledgeable and motivated. Security awareness programs are an essential element in creating such a workforce. Their revitalization is essential.

Recommendations #8, 9, and 10:

- ***Ongoing efforts to create, coordinate, and implement core national training for both Government and industry security officers should continue. The SPB needs to ensure that such a program is funded and supported, with a goal of implementation within two years.***
- ***The SPB should charter a coordinated, Government-wide security awareness program to be fully implemented within two years.***
- ***A funding line for bridge and seed money should be created to be used for initiating security training and awareness projects, and for security research initiatives, executed by designated departments or agencies.***

Cross-Cutting Issues

Security Policy Board Structure and Process

Key national security leaders perceive that the Security Policy Board process is cumbersome and unwieldy, takes too long to formulate policy, and results in spotty implementation of the policies it does put in place. These perceptions are justified.

We address in detail some important remaining obstacles to faster and more relevant progress in the following pages. However, the overarching issue is that both the daily detailed attention to long-standing security issues and the emerging issues demanding more emphasis and new innovation require the commitment of senior leadership to ensure effective and efficient security policies and practices. Part of that commitment has to be adequate resources directed at the right challenges. At present, the security profession is struggling with a downsized workforce and diminished resources while facing a more complex threat environment. The most obvious consequence of not matching resources to declared policy is the large backlog of overdue periodic reinvestigations already cited. However, there are others; for example,

> In the Department of Defense, security clearance processing is far behind schedule. Consequently, organizations are granting a record number of interim clearances. Furthermore, until recently, DoD SECRET clearances were based on National Agency Checks alone, without the Credit Checks and Local Agency Checks (of local law enforcement records) required by the standard. Since some 22 states do not report data to the National Agency data base, forgoing the Local Agency Check means that an applicant could have committed felonies in multiple states with no adverse information in the records checked.

The Defense Security Service has been unable to conduct security assistance visits to much of the industrial complex supporting the Department's facilities for several years.

Agencies have canceled core security training and awareness programs vital to addressing insider threats.

Information systems security policy remains fragmented at the managerial level, with responsibilities poorly defined and spread over multiple bodies.

The continued organization of threat analysis into specialty areas (such as separate centers for counterterrorism, counterintelligence, infrastructure protection, and so on) makes it difficult for policymakers and security professionals to obtain an accurate and usable picture of the threat to the things they are charged with protecting.

The disconnects between policy and resourced practice in both the Department of Defense and the CIA can be interpreted as signaling that the senior leadership has not been convinced that policy implementation warrants priority resourcing. Discussions with senior leaders in DoD indicate doubt that the policies are as relevant to the modern threat situation as should be the case. There have also been concerns expressed regarding the affordability of the policies, though the funding required is not of the magnitude that would raise an affordability question if senior leaders had confidence in the validity of the policies. In any case, there are obvious disconnects between the policy making apparatus and the resource allocating authorities. Since the intent was for the SPB decision process to reflect the views of these same resource allocation authorities, this raises the question of the effectiveness of the current Security Policy Board structure and process.

The Security Policy Board has been operating for over four years. Figure 1 shows the current structure.[1]

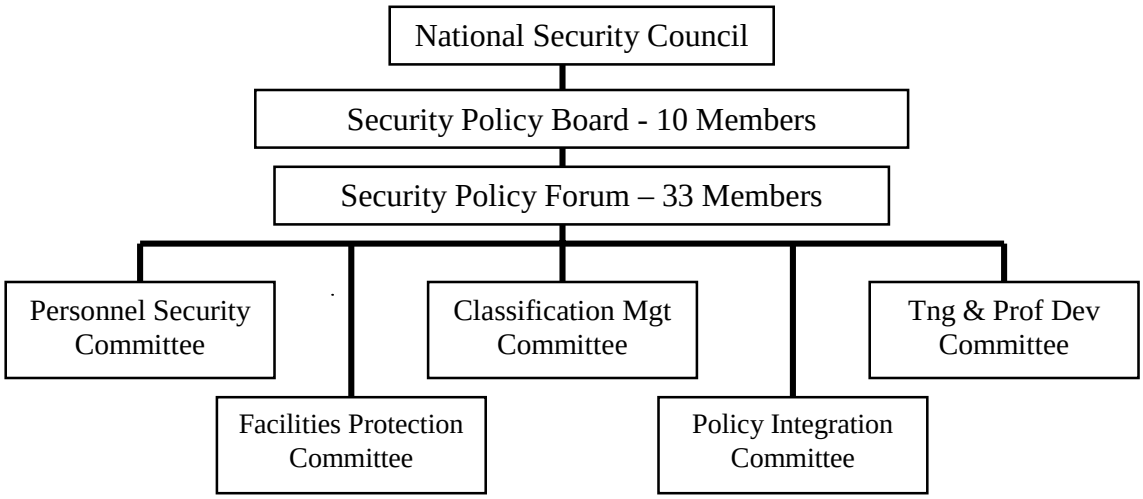

Figure 1: Security Policy Board Structure

Participants in the committees are subject-matter experts from the agencies that have an interest in a particular area. The committee members do the detailed work needed to formulate

[1] The Security Policy Forum is currently considering whether to decommission the Policy Integration Committee.

recommended policies. The Forum is composed of representatives from all the agencies involved in the security structure. The Forum meets as needed to assess the recommendation of the committees. For some issues, the Forum can approve the policy for agency implementation. For others, it passes recommendations up to the Security Policy Board, co-chaired by the Deputy Secretary of Defense and the Director of Central Intelligence and composed of senior representatives from various departments and agencies.

In our review, we found a Security Policy Board structure that is functioning at the committee level much as the original Joint Security Commission had envisioned. Furthermore, an important side benefit has proven to be the forging of positive working relationships across the Government security community, enhancing rapport and cooperation and minimizing distrust among vested interests. The Security Policy Forum has demonstrated value, though it is at this level that the desire to achieve consensus on policy formulation and approval has resulted in a process that is unwieldy, time consuming and frustrating. Hence, with the Forum often unable to resolve issues at its level, too many of them have been seen as requiring Board action. The problems of cumbersome, time-consuming processes, and spotty implementation might vanish if the Board principals exercised their decision authority on the range of issues that tend to produce stalemate in the Forum. Still, it is not surprising that they have not been willing to do this, insisting, instead, that issues brought to the Board be ones appropriate in detail and in scope of action for the level of its participants. The right solution for the Board is to empower and require the Forum to resolve the difficult issues at the right level with or without consensus.

The Security Policy Board structure is not addressing the increasingly important issues associated with greatly expanded electronic network systems or the globalization of business and technology. There is no integrated structure currently in place to address security policies associated with this class of challenges.

Restructuring the Security Policy Board

The Security Policy Forum has been particularly valuable as a means to increase the flow of information and knowledge about security matters and to create buy-in among the members. As already indicated, it has also provided the leadership needed to make important policy changes and to make significant progress towards implementation, but has done so with a high price in the time and energy expended. There needs to be a careful balance between consensus building and decision making.

Because the Forum, envisioned in PDD-29 as a body of Assistant Secretaries, has evolved into a de facto congress of Security Directors, an important management level has been effectively excluded from the security policy process. This void has, in turn, played a role in the difficulty in resolving issues at the Forum level. It has also played a role in the apparent lack of commitment to resourcing the policies. To fill this void, the Commission proposes creation of an Executive Committee, consisting of a few key players at the Assistant Secretary level. This should not be viewed as an additional layer. It is intended, instead, to be the resolution level for most issues. This Executive Committee would establish specific priorities, provide the Forum guidance as necessary, and serve as the primary avenue of communication between the Board and its subordinate structure. Working with the Board staff, the Executive Committee would be responsible for ensuring that policy initiatives, regardless of their source, do not flounder in prolonged debate, but are brought efficiently to resolution. The Forum Co-Chairs, together with the committee chairs, would jointly be responsible to the Executive Committee for day-to-day operations of the policy process.

The Commission believes that both purposes—consensus building and decision making—can be served by continuing the present membership of the Forum while creating the Executive Committee. At the call of the chair(s) of the Executive Committee, additional members with specific interests and equities could be invited to participate for specific issues.

Recommendation #11: The Security Policy Board should appoint an Executive Committee. Its members, at the Assistant Secretary level, would come from the nine agencies with permanent representatives on the Board, and would be empowered by their principals to act for them in all but the most key issues.

Under this concept, the Board would meet only to consider a few key issues. Board members would interact on matters of interest to them primarily through their empowered representative in the Forum or Executive Committee.

Changes in the security environment since 1994 generate a need for a change to composition of the Board and its scope of authority. The revolution in information technology, whose security aspects we discuss below in Part II, coupled with the increasing awareness of the need for infrastructure protection warrant adding the Deputy Administrator, General Services Administration to the Board's permanent membership, and including the Chair of the CIO Council as an observer whenever the Board discusses INFOSEC issues. The Board needs to play an active role in information technology since protecting systems involves *all* security disciplines, and only the Board and its subordinate structure are placed to achieve the necessary fusion.

Recommendations #12 and 13:

- ***The Deputy Administrator, GSA should be added as a permanent member of the Board; the Chair, CIO Council should attend all meetings and be involved in Board activities addressing INFOSEC issues.***
- ***The Board's charter should be modified to clarify its role in INFOSEC and its relationship to the NSTISSC.***

<u>The Concept of Risk Management</u>

The basic concept for a cost effective security system is risk management rather than the unattainable and unaffordable goal of risk avoidance. However, the concept of an effective and affordable system based on risk management assumes an understanding of the threat, the capability to measure the cost, and some means of measuring the risk. At present, there is little reliable analytical data for any of these parameters. Instead, the focus is on the cost of some specific sub-element of security practices without consideration of the impact on other security costs or on risk. Some specific examples are discussed in following sections.

Understanding the Threat

Recognition of the need for a better approach to understanding the threat led to creation of the National Counterintelligence Center (NACIC). The NACIC has made significant strides toward facilitating the flow of information to those cleared individuals who use it daily to form security countermeasures. However, for those seeking an authoritative source of available relevant threat intelligence, the picture is more complex. Diverse areas of concern include espionage, terrorism, threats to critical infrastructures and environmental safety, information/cyber warfare, illicit technology transfer, drug and other international crime organizations, and intellectual property fraud. Multiple infrastructures of intelligence producers, disseminators, and users—spread across agency lines—provide threat products.

This fragmentation has made it significantly more difficult for the security countermeasures community, both Government and industry, to obtain timely and accurate threat data. The most effective way to overcome this fragmentation is through a single organization designated to provide customers from the cleared community with one central location for their threat intelligence needs. The National Counterintelligence Center today has as its area of responsibility the dissemination of foreign counterintelligence information. Given additional resources and responsibility, it could become a community reference center that would provide consolidated threat data or, as a minimum, refer customers to sources of other kinds of threat data relevant to their needs. In conjunction with an expanded NACIC, advancing technology provides other possibilities for disseminating threat information, such as computerized pull-down systems that would provide data when the user needs it.

An expanded NACIC should also be given greater responsibility for providing meaningful threat information to industry partners. Both Government and industry officials have information they do not often share with one another. If the NACIC adopted a more collaborative approach whereby it consulted regularly with industry officials, the few classified threat *briefings* the NACIC now provides could turn into more useful threat *seminars*, providing both Government counterintelligence officials and industry security representatives with better two-way communication. This would allow both parties a far better understanding of the range of current problem sets and how to defend against the threat in a consolidated manner.

In April 1997 an interagency group chartered by the SPB to identify and address the process of threat dissemination issued its coordinated *Comprehensive Intelligence Production Requirements Statement in Support of Security Countermeasures Consumers*, identifying intelligence items relevant to specific security needs. It was intended as a first step in developing an effective, efficient process and dialogue supporting dissemination of threat intelligence information. While it has proven helpful, there is much more potential in the group's work. The National Security Advisor, giving formal recognition that it reflects the needs of the security community, should issue the document. Once this is done, the process and infrastructure necessary for meaningful dissemination of threat data need to be more fully addressed.

Recommendations #14 and 15:

– ***Charter, fund, and staff the NACIC as the single clearinghouse for threat information for the security community.***

– ***The Security Policy Board should formally request the National Security Advisor to issue the*** **Comprehensive Intelligence Production Requirements Statement in Support of Security Countermeasures Consumers.**

Understanding the Cost

As the Commission pointed out in its 1994 report, the cost of security is an elusive target. It remains so today. The Commission believes limited progress has been made, however. In 1994, responding to a House Appropriations Committee tasking, OMB first captured security cost estimates for safeguarding classified information within the Executive Branch. During 1994-95, the Security Policy Board developed a framework for estimating all security costs, not just those associated with the protection of classified information. Beginning in 1995, this framework was adapted to collect security cost estimates for protecting classified in the Executive Branch on an annual basis as required by EO 12958.

However imperfect, the annual cost reporting under EO 12958 is the most broadly applicable, if not the sole measure, of security costs to Government. Additional partial indicators of the costs of security are the special authorizations for FY99 totaling $12.2 billion. Of this amount, $2.8 billion has been authorized for computer security and biological warfare defense, $8 billion for physical security of embassies around the world, and $1.4 billion for critical infrastructure protection. Also, while not a measure of the costs of security, the exigency funding for Y2K is a rare example of spending for other priorities that will incidentally benefit security.

We see several important limitations threatening continuing progress toward accurate security cost accounting. The most important is that few Executive Branch departments and agencies have separate budget line items for security. In many cases, security resources are included in overhead accounts. Additionally, differentiating security costs related to classified and unclassified matters is problematic because security personnel and physical assets typically contribute to both realms simultaneously. OMB recognized that initial reports for the EO 12958 annual collection would be estimates at best, and that the data could not initially be audited. OMB hoped that over time the data would become more credible through repetition and familiarity with the collection parameters and refinement of collection techniques. In fairness, however, we note that there has been no follow-up measurement to ensure applying appropriate rigor to these annual collections or doing them on a department/agency-wide basis. This means that problems of comparability due to widely varying systems, security data standards, and data reliability among agencies limit the accuracy and completeness of current reporting. Furthermore, there is generally no tie-in between agency security budgets and execution of national security policies. A commitment to collect security costs by functional category against the framework developed by the SPB would overcome this shortcoming and would permit establishing, in each agency, separate budget lines for security, which would provide a straightforward and readily understandable answer to questions of security costs.

Fee-for-service has a role to play as a means for clearly delineating costs. However, the attempt to implement it concurrently with the present set of challenges facing the Defense Security Service has proven too difficult. Until DSS can fully achieve base standards and aggregate costs can be determined, fee-for-service should be tabled. Successful implementation

will include a cost accounting system that recognizes security's command function and deemphasizes its administrative role.

Given today's budgeting practices, and varied perspectives on what security means, there is no one simple answer to the question, "How much do we spend on security?" Post-Cold War notions abound that "security costs too much" or that a "peace dividend" should be found by decreasing security resources to match supposedly diminished threats. Such notions are simplistic and misinformed. Whatever its effect on our national security, the loss of the popular notion of a single, all-encompassing threat has only obscured the emergence and proliferation of often less restrained and more virulent security threats. Such novel challenges require vastly different security countermeasures prescriptions, for which the resource implications remain undefined.

Recommendations #16 and 17:

- ***The SPB should mandate collection of all security costs against the security cost framework already developed.***
- ***Agencies should call out security as a separate line item in their annual budgets.***

Security Policy Board Staff Position Funding

The Commission found that assignments to the SPB Staff during the first four years of the Board's existence generally worked well to promote the SPB's mission. Personnel detailed to the Staff brought wide-ranging experience and expert practitioner knowledge to the policy making process. However, the informal nature of the commitment creates turbulence and adversely affects Staff functions. The SPB should be supported with funded staff positions.

Recommendation #18. Provide funded Security Policy Board Staff positions and contractor support where needed.

The Extranet for Security Professionals

Effective security that has reciprocity as a key component requires effective communications among those responsible for administering it. Such communications are important for activities ranging from policy coordination to rapid announcement of changes to day-to-day tasks such as clearance passing and access verification. The Extranet for Security Professionals (ESP), currently experimental, provides a vehicle for such communications. The experiment is proving successful. ESP holds particular potential for resource savings through providing clearance and visit certification throughout Government and industry. Full development and continued operations and maintenance resourcing of the ESP, with attention to providing confidence in its future, should greatly expand its use and ensure the continued availability of what should prove to be an essential tool for more effective security.

Recommendation #19: The SPB should continue to support the ESP, ensuring its continued development, funding, and eventual operational status.

Industrial Security

Including industry observers in the committees and at the Forum has facilitated a dialogue between industry and Government that has proven beneficial to both. Industry is and will remain a critical contributor to national security. As such, it is important that the dialogue continue, but not merely at the policy level. DSS security assistance visits play an important role in ensuring effective security programs, both by serving as a means for identifying problems and potential problems and by conveying to management that the Government continues to place value on security. Yet DSS's ability to conduct these visits has eroded to the point that they have become sporadic: still good in some areas, but nonexistent in others. Industry continues to suffer from excessive backlogs in the clearance process that delays putting people to work. The Government suffers as this slows progress on classified projects and ultimately drives up costs. At the same time, the proposed program calling for industry to convert to the XO7 lock threatens to add additional costs without a commensurate increase in security. The estimated cost to implement the mandate in just five of the many Defense Companies is $24M for retrofit and $92M for lockbar conversion. Given the absence of a credible threat to the security of current containers in the continental US, money that would be spent on XO7 conversion could be better spent to augment the DSS industrial security program and to provide at least some of the wherewithal for expediting the personnel security process for industry.

There has been a notable lack of progress since 1995 in producing usable INFOSEC guidance for the defense industry. Chapter 8 of the NISPOM baseline is mired in disagreement between major players—DoD, CIA, and DoE. This situation creates a vacuum in an area that urgently needs effective, up-to-date security policy. Of particular importance is the issue, as yet unresolved, whether the document should be performance-based or prescriptive. Policy uniformity and consistency of implementation must be elements of all INFOSEC guidance. The continued inability to provide guidance to industry is creating enormous frustration in industry and weakens national security INFOSEC programs. This is an issue deserving and demanding the attention of the senior leadership in information systems security. The NISPOM must become, as it was intended, the single governing document for the industrial security program.

Recommendations #20 and 21:

- ***The Deputy Secretary of Defense should immediately put the Defense Security Service on a footing to revitalize the program of industrial security visits and to provide timely background investigations that meet the agreed-to guidelines.***
- ***The Security Policy Board Co-Chairs should require that the Executive Committee provide the full Security Policy Board an agreed-to baseline Chapter 8 for approval within 180 days.***

Overseeing Compliance—A Need Overlooked

PDD-29 assigns the SPB the responsibility for formulating and coordinating policy. It is, however, silent about mechanisms for oversight of implementation. EO 12958 charters the ISOO, but circumscribes its area of responsibility and does not address resources for it. Other relevant documents, including EO 12968, PDD-63, and OMB Circular A-130, do not provide for national-level oversight.

There is internal agency oversight, and it is essential; however, no effective mechanism is in place today to monitor policy implementation for coherence and consistency, and to ensure that policies are applied equitably and in ways consistent with national goals for standard security policies and interagency reciprocity. Such oversight is not a matter of compliance inspections, but a matter of consultative review at the policy level, designed to ensure that policy is practical, understandable, and addresses real issues, and to identify and resolve implementation issues. The SPB should establish a process for timely reporting of progress towards compliance by all agencies. The SPB is well positioned to assume this national-level oversight role.

Contributing to the general problem of oversight of implementation is the lack of a clearly defined and broadly accepted mechanism for the Security Policy Board to issue its decisions. Once the Board approves a policy, and even when a policy is endorsed in a memorandum from the National Security Advisor, there is no definitive way to institutionalize that policy for the Government as a whole. This shortcoming could be easily overcome by creating a recognized and recognizable series of binding policy documents.

Recommendations #22 and 23:

- ***Clarify the role of the SPB in national level security policy oversight, reemphasizing the SPB as the primary oversight body.***
- ***Establish a recognized mechanism for promulgating SPB decisions.***

PART II: SECURING INFORMATION SYSTEMS

The goal of INFOSEC is to ensure that the National Security Community has reliable and secure networks to originate, store, manipulate, and make information available to those who need it and are authorized to have it. INFOSEC enables readiness. It must do this in a rapidly changing and increasingly more complex technical environment, against threats that are evolving and not well understood, and with a structure of authorities that is still emerging and coalescing. This part of the Commission's report recommends an approach to INFOSEC that, if implemented, will provide a coherent framework for dealing with present and future challenges.

Organizing INFOSEC in the Government

The structure of authorities for INFOSEC in the Government requires clarification and coherence (see Figure 2). An example of the need for increased coherence is found in the Computer Security Act of 1987. It was the first legislation to bind computer and telecommunications resources under a single definition. It also created multiple organizations and divided responsibilities and authorities for information systems security.

The Act emanated, in 1984, from HR-145, a bill intended to nullify National Security Decision Directive (NSDD)-145. NSDD-145 created the National Telecommunications and Information Systems Security Committee (NTISSC) as the *national* authority for information systems security. NTISSC's authority covered both classified and unclassified systems for Government and extended into the private sector. Under NSDD-145, the Secretary of Defense served as the Executive Agent for the Government in national telecommunications and information systems security matters, and the Director of the National Security Agency was the National Manager for such matters. The Chairman of the House Government Operations Committee was opposed to the defense and intelligence community role assigned by NSDD-145, declaring that it violated First Amendment freedoms. HR-145 was enacted into law as PL 100-235, on January 8, 1988. It greatly reduced the role and effectiveness of the NTISSC.

PL 100-235 amended the Brooks Act, which had conferred on OMB responsibility for "fiscal and policy oversight" of the powers assigned to GSA, NIST, and OPM. In matters of information system technology, this authority evolved first, in the Paperwork Reduction Act, into "providing direction and overseeing," and ultimately became, in the Clinger-Cohen Information Technology Management Reform Act, "directing and controlling" the agencies.

The one area of clear agreement is that INFOSEC plays a vital role in national security and in the Critical Infrastructure. Hence, PDD-63 proposed partnering relationships including the Critical Infrastructure Assurance Office (CIAO), the National *Security* Telecommunications and Information Systems Security Committee (NSTISSC), and the US Security Policy Board. CIAO also partners with NIST, OMB, and the Chief Information Officer Council (CIOC) in critical infrastructure matters. The CIOC, authorized by the Clinger-Cohen Act, has established a goal of Government-wide integration, under its auspices, of information technology policy development in coordination with OMB. At a recent briefing to the Computer System Security and Privacy Board, the CIO Security Committee presented a strategic vision of coordinating and integrating existing security groups, assessing and directing ongoing security efforts, and

leveraging existing security group resources. The CIOC is currently collaborating with the CIAO and OMB in formulating a budget for INFOSEC across the Government.

This "everyone is in charge" arrangement means that no one has responsibility for meeting the vital needs for INFOSEC for national security. The OMB, NIST, NSTISSC, and CIOC authorities for INFOSEC are *Government-wide.* At the same time, the SPB is assigned authority and responsibility by PDD-29 and the DCI's authority for DCIDs. Figure 2 attempts to illustrate the fragmentation of authority and function.

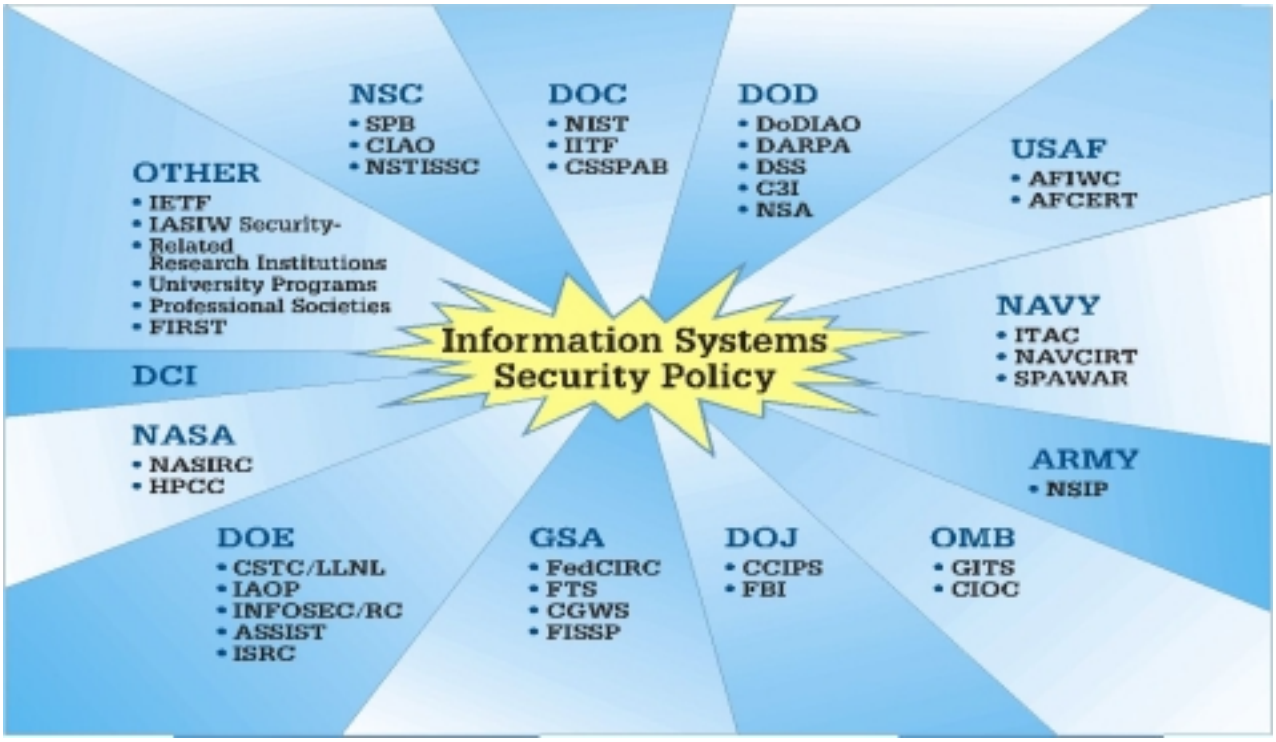

Figure 2: The INFOSEC Policy Structure

There is an urgent need for direction that recognizes the changes in information systems technology over the past decade and the role it plays in national security. The original Computer Security Act was enacted at a time when there was no foreseeing today's global information infrastructure or its importance to national security. Networks were rudimentary and segregated. Implementing directives for the Computer Security Act of 1987, OMB Bulletins 88-16 and 90-06, were suitable for remote batch processing technology. Their later incorporation into the revision of OMB Circular A-130, Appendix 3, leaves us with an urgent need for policies suitable to the modern and constantly changing technological model.

The vision of the CIO Council to join the fragmented INFOSEC leadership in partnership with OMB will have the proper focus only if it treats the growing global information infrastructure as the model—the *common* carrier of *classified and unclassified* image, data, and voice information through virtual circuits, globally integrated under the control of computers designed and programmed to function as network controllers and switches. This is the holistic reality that must drive the policies, processes, and mechanisms to bring about real world structures and processes that can assure the reliable flow of uncompromised information between, and only between, legitimate senders and intended receivers. The needed holistic

global policy approach leaves no room for fragmentation of authority and responsibility among parochial constituencies.

As an example of the conflict that is inevitable among splintered constituencies, OMB Circular A-130, Appendix 3, Section 4.f. "assigns" the Security Policy Board responsibility for *national security* policy coordination, including policy for the security of information technology used to process *classified* information. However, PDD-29 assigns the responsibility without limiting it to policy for national security or technology used to process *classified* information. This "assignment" perpetuates the fragmentation of responsibility and authority to provide effective protection of mission critical information and information systems regardless of classification.

Recommendation #24: The Deputy Secretary of Defense and Director of Central Intelligence, working with the National Security Advisor and Director of the Office of Management and Budget, should resolve the issue of national authorities for INFOSEC and propose a presidential directive (and legislation if appropriate) to implement their solution.

Defense in Depth

The widely recognized defense-in-depth model for INFOSEC is "detect-protect-respond." However, the Commission found that most of the attention and investment is devoted to the "protect" aspect with reduced attention to "detect" and little attention to "respond." What attention we did find to "respond" tends to be forensic in nature—that is, intended to discover the means used to penetrate the system to strengthen the protection. Yet we must design the security of our systems so that they continue to meet critical needs even—perhaps especially—when under attack.

In contrast to the "detect-protect-respond" model, we strongly support the "resist-recognize-recover" model described by the Computer Emergency Response Team at Carnegie-Mellon. In this context, "resist" means to raise the barriers against attacks to the highest practical, affordable level, but to do so with the understanding that sophisticated attackers are likely to breach barriers that still permit data flow outside some closed system. Further, experience to date is that the greatest damage comes from insiders. Hence it is essential that the information system be designed to control the damage from breaches by external attacks or from malicious or careless insiders. Hence, there is a need to engineer into the system the means of monitoring what is going on within the network—who is in the system, where is information flowing, what is happening to the data in the system, what is happening to the system. This kind of monitoring is essential both to protect the security and integrity of the information and to protect against denial of services that are essential to national security operations. Monitoring, however, is not an end unto itself, but is a tool. Accountability—of the system administrator, of the agency head, and of everyone in between—remains paramount. Technology alone is helpless to solve the INFOSEC problem.

It is equally important in designing secure systems to assume that sophisticated attackers or malicious insiders will find ways to do great harm to the functioning of the system. Hence

rapid recovery capabilities need to be engineered into critical systems—classified or unclassified. With the great strides forward in information system performance and with the rapidly growing dependence on such systems for all kinds of national security operations, it is now essential that all critical system design requirements include specific provisions for engineering in information system monitoring and recovery. These three levels—resist attack, detect anomalies within the system in time to control the damage, and built-in rapid recovery—constitute the needed defense in depth. The solution is a combination of technical methods and security practices and procedures, to include substantive information systems security training, education, and awareness.

Further, with system performance reaching levels that meet or exceed most users' needs, and with the growing awareness of the potential damage from malicious intruders or insiders, there is increasing commercial interest in network defense and an increasing flow of products advertised as contributing to network defense. There is also an increased willingness in the commercial sector to work with the Government to address these critical needs. In particular, there is rapidly growing interest in the finance and banking, telecommunications, energy, and information technology sectors. However, the Commission found no organized approach to partner with the commercial sector or to seek out and evaluate commercial products though an increasingly wide range of such products are in use in various parts of the Government.

One element that has helped enable outsiders to hack systems is their anonymity. The difficulty in identifying the precise source of an attack reduces the range of potential defenses while bestowing on the hacker considerable scope for operation. Removing this anonymity through creation of the electronic equivalent of fingerprints is a technological problem whose solution would prove of significant INFOSEC benefit.

Fundamental to defense in depth is the Government's inherent right to protect its information systems. Defense in depth is to ensure that the national security community can continue to conduct its business. The first responsibility is to protect that which is defended—to minimize damage and to continue to ensure system operation. Catching criminals is important, but never at the expense of protecting the information and the systems that are essential to national security operations.

Recommendations #25, 26, 27, and 28:

- ***The Department of Defense should vigorously pursue defense-in-depth funding, leveraging the growing private interest in such efforts and leading the investment needed to adequately monitor and audit information systems to detect anomalies and respond quickly to control damage.***
- ***The Deputy Secretary of Defense should take immediate steps to mandate an architecture for the Department's critical information systems that includes specific requirements for designed-in monitoring and auditing and provisions for rapid recovery and continued operation in the face of sophisticated attacks or malicious insiders whose purpose is massive compromise of information or denial of service. Such an architecture would leverage current initiatives such as DoD's Public Key Infrastructure Roadmap and work on X.509 certificate policy.***
- ***Available means of raising the barriers to system penetration should be vigorously and rigorously pursued and applied—certifications, tokens, and encryption.***

– ***The Deputy Secretary of Defense should take the lead in establishing a research and development effort that focuses on partnering with commercial interests, exploiting commercial tools, and developing special purpose DoD state-of-the-art tools for recognizing and responding to attacks against information systems.***

The Threat from the Inside

The potential for insider damage deserves special attention. Personnel security practices have long focused on attempting to deal with the dangers posed by the trusted insider who chooses to do harm. The potential for devastating damage is exponentially greater in an information technology environment. Instead of stealing a few documents at a time, the traitor within can now walk away with the contents of an entire system, or write a few lines of code that surreptitiously corrupts critical data or blatantly destroys a network.

Resist-recognize-recover applies equally to the inside threat. The first line of defense against the insider is the classic personnel security model of investigation and monitoring. And, in the case of particularly sensitive programs, the standards for investigation and monitoring are appropriately higher. System administrators, by virtue of the exceptionally important role they play—as positive forces for protection, or negative forces for damage—should receive greatly increased attention. Their special situation warrants more stringent investigations, closer monitoring, limitations on individual authorities, and stringent certification and continuing training.

Specifically, restricting root access to those few who *must* have it to ensure system operation would minimize the most serious vulnerability of a system to the insider. Even then, a two-person process should be considered for such root access. As a matter of principle, no one person should have all the system accesses necessary to shut down or to access an entire system. The two-person rule has long been in use for access to nuclear weapons. Cyber systems have become at least as important to national security as nuclear weapons and the potential for damage to national security rivals that of nuclear weapons.

Recommendations #29 and 30:

– ***The Director of Central Intelligence and the Deputy Secretary of Defense should establish rigorous clearance, monitoring, certification, and continuation training standards for system administrators.***

– ***The Director of Central Intelligence and Deputy Secretary of Defense should reduce the number of people holding root access to their systems to the irreducible minimum, and require that all such accesses follow the two-person rule similar to that used for access to nuclear weapons.***

An added risk of compromise comes from the simultaneous need for frequent upgrades, complex system configuration processes, and the need for rigorous configuration control to ensure that the designed in security provisions can provide the intended level of protection. A single unauthorized modem can compromise an entire system. Today, we find common viruses on the SIPRNET indicating unauthorized introduction of disc-based programs onto computers on

the Internet. Each such unauthorized introduction carries the risk of a compromise to the system. Automatic processes for upgrades and rigorous configuration control are essential elements of information system security.

Recommendation #31: The Deputy Secretary of Defense should require that system design include provisions for automatic upgrade of system security features and rigorous control of applications on critical networks.

The threat from the inside can also reside in products. The Government has no choice but to rely heavily on commercial off-the-shelf products for its information technology needs. However, these products do introduce a degree of risk. Whether a given operating system or other piece of software contains malicious code or an exploitable weakness is difficult if not impossible to determine. We cannot eliminate the risk, but must recognize it and maintain vigilance to the extent possible, exercising the caution consistent with the model of "resist-recognize-recover" already described. As a minimum, working with commercial software developers to ensure disclosure of foreign content in software is desirable, since foreign content is one potential source of security concern. The joint NIST-NSA National Information Assurance Partnership (NIAP) provides a mechanism for addressing security issues in commercial products, but thorough security testing is time-consuming and frustrated by both the rapid changes to existing software and the large number of products entering the market that are the computer industry's norm. Research into advanced tools that can effectively and efficiently evaluate products as they are developed and as they evolve, if successful, would provide the Government a critical tool for increasing the level of security confidence in the products it deploys.

Recommendations #32 and 33:

- ***The Deputy Secretary of Defense should develop a means for ensuring that commercial software developers certify foreign content of all software purchased by the Department of Defense.***
- ***The Deputy Secretary of Defense should further support a research effort, building on the work of the NIAP, that would lead to advanced tools to evaluate commercial computer products to be used by the Government.***

Training the Information Technology Professional

There are too few system administrators and even fewer who are fully qualified. With the increased dependency on information systems, it is increasingly important that those individuals responsible for the operation and maintenance of our information systems be well qualified. Yet, frequently, the job is performed as an additional duty or by individuals without the required background and training. Many, lacking the requisite skills for their tasks, are overwhelmed just keeping their systems up and running. A culture demanding that customer desires for performance take precedence over security creates additional vulnerabilities,

particularly when system administrators are inadequately trained junior people. Poorly trained and overworked systems administrators constitute a security threat, not from maliciousness, but from ignorance. To the operator in the field, it makes little difference whether a critical system failed because of a hostile penetration or because an untrained systems administrator made it vulnerable to a destructive attack.

The Government by itself cannot create the IT professionals it requires, nor by itself provide them with the INFOSEC grounding they need to do their jobs effectively. The Federal Information Technology Service initiative—commonly referred to as "Cybercorps"—which trades undergraduate financial aid for commitment to work for the Federal Government upon graduation, is a prototype for Government-university cooperation, but it remains unfunded. Another alternative would be establishing programs under the auspices of the Corporation for National Service, established by the National and Community Service Act of 1993, in colleges for computer science and information systems security expertise.

Currently, the Government finds it difficult to compete for talented computer experts because the salaries it pays are well below those found in industry. Professionalizing the field by creating its own career service with appropriate grade scales, may be a viable approach to recruit and retain the people it requires.

One way of attracting highly qualified, highly motivated people would be to create a state-of-the art national laboratory that would work leading-edge technologies for the Government. Such a laboratory would create the solutions to unique DoD and Intelligence Community information technology security problems, developing products and approaches to improving security features on a system basis.

Recommendations #34, 35, and 36:

- ***The SPB should formally ask the President to fund and implement a Cybercorps-like program.***
- ***The SPB should create a task force, chaired by OPM and with the support of the CIO Council, to work toward creating a separate career field for INFOSEC professionals, with requisite education, training, and certification requirements and a grade structure that competes favorably with industry for the same talent pool.***
- ***The SPB should formulate to the NSC a recommendation to create a national INFOSEC laboratory that would become the center for creating advanced solutions to unique Government IT security issues and for advancing the state of the art.***

CONCLUSION

In the five years since the original Joint Security Commission issued its report, a great deal has occurred to change the security landscape. The Security Policy Board structure has been instrumental in forging cooperation among disparate agencies where before distrust was normal. Its processes, particularly at the top, are cumbersome; however, it provides the one available structure for ensuring Government-wide solutions to problems that are no longer the exclusive concern of the defense and intelligence communities. The changes recommended in this Report should both retain the benefits provided by the Security Policy Board structure and improve its effectiveness.

Information technology has transformed the Government's ways of doing business (including the business of war), and is transforming the relationship between the public and private sectors. The current structure of authorities for protecting this technology is incoherent and self-defeating. INFOSEC professionals, lacking clear national-level guidance, are struggling with inadequate models. Attention to the question of authorities and recognition of the value to be gained through a resist-recognize-recover model of defense in depth are the minimum starting points necessary to ensure that critical systems will continue to be available to the nation.

Annex A

Summary of Joint Security Commission II Recommendations

Reliable and Trustworthy People

- Recommendation #1: The Co-Chairs of the Security Policy Board, leveraging efforts already contemplated or underway, should commission and fund a research effort to determine the efficacy of personnel security policies and to resolve issues about their effectiveness. The Co-Chairs should monitor this effort, ensure the proper assessment of its results, and use those results to develop appropriate policies.
- Recommendation #2: DoD should reassign SRC to OASD C^3I; moreover, DoDPI should be redesignated the National Polygraph Institute with the Security Policy Board designated the National Manager and DoD OASD/C^3I the Executive Agent.
- Recommendation #3: The Department of Defense should begin first to fully enforce the standards for reinvestigations and then, within 90 days, should screen all overdue for reinvestigation to identify those whose positions and access suggest the highest risk, and should provide the resources to complete those reinvestigations promptly; the Central Intelligence Agency should expeditiously execute its plan to eliminate its backlog by 2000.
- Recommendation #4: DoD and CIA should set a limit of 180 days for new Interim clearances, requiring that the needed background checks and adjudication process be completed within that period. In addition, they should screen all existing Interim clearances and promptly close out those where positions and access suggest the highest risk.
- Recommendation #5: The Security Policy Board should maintain a high priority on applying common standards to Special Access Programs and require that any needed policy recommendations go from the SPB to the NSC within 180 days.
- Recommendation #6: DoD should immediately provide adequate funding and field a SAP access database, with appropriate security controls, to facilitate effective reciprocity.
- Recommendation #7: The Board should propose to the NSC a new Executive Order that takes a comprehensive approach to addressing the suitability, reliability, and trustworthiness of persons employed in sensitive duties on work for the federal government. This would include individuals working in any capacity, and based upon the sensitivity of the duties, regardless of access to classified information. A proposal from the Security Policy Board for such an order is consistent with its stated mission in PDD-29.

Education, Training, and Awareness, and Accountability

- Recommendation #8: Ongoing efforts to create, coordinate, and implement core national training for both government and industry security officers should continue. The SPB needs to ensure that such a program is funded and supported, with a goal of implementation within two years.

- Recommendation #9: The SPB should charter a coordinated, government-wide security awareness program to be fully implemented within two years.
- Recommendation #10: A funding line for bridge and seed money should be created to be used for initiating security training and awareness projects, and for research initiatives, executed by designated departments or agencies.

Restructuring the Security Policy Board

- Recommendation #11: The Security Policy Board should appoint an Executive Committee. Its members, at the Assistant Secretary level, would come from the nine agencies with permanent representatives on the Board, and would be empowered by their principals to act for them in all but the most key issues.
- Recommendation #12: The Deputy Administrator, GSA should be added as a permanent member of the Board; the Chair, CIO Council should attend all meetings and be involved in Board activities addressing INFOSEC issues.
- Recommendation #13: The Board's charter should be modified to clarify its role in INFOSEC and its relationship to the NSTISSC.

Understanding the Threat

- Recommendation #14: Charter, fund, and staff the NACIC as the single clearinghouse for threat information for the security community.
- Recommendation #15: The Security Policy Board should formally request the National Security Advisor to issue the ***Comprehensive Intelligence Production Requirements Statement in Support of Security Countermeasures Consumers***.

Understanding the Cost

- Recommendation #16: The SPB should mandate collection of all security costs against the security cost framework already developed.
- Recommendation #17: Agencies should call out security as a separate line item in their annual budgets.

Security Policy Board Staff Position Funding

- Recommendation #18: Provide funded Security Policy Board Staff positions and contractor support where needed.

The Extranet for Security Professionals

- Recommendation #19: The SPB should continue to support the ESP, ensuring its continued development, funding, and eventual operational status.

Industrial Security

- Recommendation #20: The Deputy Secretary of Defense should immediately put the Defense Security Service on a footing to revitalize the program of industrial security visits and to provide timely background investigations that meet the agreed-to guidelines.
- Recommendation #21: The Security Policy Board Co-Chairs should require that the Executive Committee provide the full Security Policy Board an agreed-to baseline Chapter 8 for approval within 180 days.

Overseeing Compliance - A Need Ocerlooked

- Recommendation #22: Clarify the role of the SPB in national level security policy oversight, reemphasizing the SPB as the primary oversight body.
- Recommendation #23: Establish a recognized mechanism for promulgating SPB decisions.

Organizing INFOSEC in the Government

- Recommendation #24: The Deputy Secretary of Defense and Director of Central Intelligence, working with the National Security Advisor and Director of the Office of Management and Budget, should resolve the issue of national authorities for INFOSEC and propose a presidential directive (and legislation if appropriate) to implement their solution.

Defense in Depth

- Recommendation #25: The Department of Defense should vigorously pursue defense in depth funding, leveraging the growing private interest in such efforts and leading the investment needed to adequately monitor and audit information systems to detect anomalies and respond quickly to control damage.
- Recommendation #26: The Deputy Secretary of Defense should take immediate steps to mandate an architecture for the Department's critical information systems that includes specific requirements for designed-in monitoring and auditing and provisions for rapid recovery and continued operation in the face of sophisticated attacks or malicious insiders whose purpose is massive compromise of information or denial of service. Such an architecture would leverage current initiatives such as DoD's Public Key Infrastructure Roadmap and work on X.509 certificate policy.
- Recommendation #27: Available means of raising the barriers to system penetration should be vigorously and rigorously pursued and applied—certifications, tokens, and encryption.
- Recommendation #28: The Deputy Secretary of Defense should take the lead in establishing a research and development effort that focuses on partnering with commercial interests, exploiting commercial tools, and developing special purpose DoD state-of-the-art tools for recognizing and responding to attacks against information systems.

The Threat from the Inside

- Recommendation #29: The Director of Central Intelligence and the Deputy Secretary of Defense should establish rigorous clearance, monitoring, certification, and continuation training standards for system administrators.
- Recommendation #30: The Director of Central Intelligence and Deputy Secretary of Defense should reduce the number of people holding root access to their systems to the irreducible minimum, and require that all such accesses follow the two-person rule similar to that used for access to nuclear weapons.

- Recommendation #31: The Deputy Secretary of Defense should require that system design include provisions for automatic upgrade of system security features and rigorous control of applications on critical networks.
- Recommendation #32: The Deputy Secretary of Defense should develop a means for ensuring that commercial software developers certify foreign content of all software purchased by the Department of Defense.
- Recommendation #33: The Deputy Secretary of Defense should further support a research effort, building on the work of the NIAP, that would lead to advanced tools to evaluate commercial computer products to be used by the Government

Training the Information Technology Professional

- Recommendation #34: The SPB should formally ask the President to fund and implement a Cybercorps-like program.
- Recommendation #35: The SPB should create a task force, chaired by OPM and with the support of the CIO Council, to work toward creating a separate career field for INFOSEC professionals, with requisite education, training, and certification requirements and a grade structure that competes favorably with industry for the same talent pool.
- Recommendation #36: The SPB should formulate to the NSC a recommendation to create a national INFOSEC laboratory that would become the center for creating advanced solutions to unique Government IT security issues and for advancing the state of the art.

Annex B
List of Joint Security Commission-II
Commissioners and Support Staff

Commissioners	Larry D. Welch, *Chairman*	
	Duane P. Andrews	
	Robert F. Behler	
	Thomas A. Brooks	
	J. Robert Burnett	
	Ann Caracristi	
	Antonia H. Chayes	
	Cynthia P. Conlon	
	James J. Hearn	
	Bernard A. Lamoureux	
	Anthony A. Lapham	
	Frank K. Martin	
	James R. Philblad	
	Dan Ryan	
	Ross E. Schipper	
	Nina J. Stewart	
	Harry A. Volz	
Staff	Dan L. Jacobson, *Executive Director*	Navy
	Edward S. Wilkinson, Jr., *Deputy Executive Director*	CIA
	Wayne Belk	Air Force
	Christopher Bythewood	NSA
	Gary Gower	State
	Gary Harris	CMS
	Doug Hinckley	CIA
	Joseph Holthaus	CIA
	Willard Isaacs	DoD/DSS
	Virginia (Ginna) Kerry	NSTISSC
	Daniel Knauf	NSTISSC
	Ray LaVan	Treasury
	Winiferd (Winnie) Lehman	Energy
	Stephen MacKnight	Navy
	Dan McGarvey	NRO
	William Mussen	DIA
	James Passarelli	Army
	Roger Schwalm	CIA
	Dave Stevens	NSA
	Administrative, Secretarial and Clerical Support:	
	Annette Purcee	CIA
	Phyllis Norling	Navy
	Deborah Jermunson	IDA

Annex C

Summary Status of Joint Security Commission I Recommendations

Rec #	Recommendation	Implementation / Status
JSC_001	One-level classification system with 2 degrees of protection.	Secs 1.3 & 4.2 of EO 12958 issued 20 Apr 1995, retains three levels of classification: Top Secret, Secret, and Confidential.
JSC_002A	Integrate all special access, SCI, covert activities etc. into the new classification system.	EO 12958 issued 20 Apr 1995, did not require the integration of all controlled access activities.
JSC_002B	Combine all special control channels into a single channel with codewords for need-to-know lists.	EO 12958 issued 20 Apr 1995, rejected JSC recommended classification system. However, agencies have made important progress, and continue to seek fewer categories under more integrated special access and compartments, in response to initiatives by the SPB.
JSC_003	Review and validate categories of sensitive information for inclusion under the secret compartmented access control system.	Implemented through DepSecDef Memorandum, dated 5 Jan 1994 and DCID 3/29, dated 2 Jun 1995. The DCIs CAPOC, DOEs SAPOC and DoDs SAPOC review and validate the categories of sensitive information included in SCI programs and NFIP-funded SAPs and Restricted Collateral programs.
JSC_004	Managers shall review information within compartments/ subcompartments and consolidate into the fewest possible compartments.	Implemented through DepSecDef Memorandum, dated 5 Jan 1994 and DCID 3/29, dated 2 Jun 1995. The DoD' SAPOC, DOEs SAPOC and the DCIs CAPOC accomplish the review recommended on a continuing basis.
JSC_005	Establish uniform risk assessment criteria.	Implemented through DepSecDef Memorandum, dated 5 Jan 1994. and DCID 3/29, dated 2 Jun 1995. The DoDs SAPOC, DOEs SAPOC and the DCIs CAPOC accomplish the review recommended on a continuing basis.
JSC_005B	Conduct independent risk assessments of compartmented access programs.	Implemented through DepSecDef Memorandum, dated 5 Jan 1994 and DCID 3/29, dated 2 Jun 1995. The DoDs SAPOC, DOEs SAPOC and the DCIs CAPOC accomplish the review recommended on a continuing basis.
JSC_005C	Across DoD and the IC, review similar compartmented access programs to ensure reciprocity.	Implemented through DepSecDef Memorandum, dated 5 Jan 1994 and DCID 3/29, dated 2 Jun 1995. The DoDs SAPOC, DOEs SAPOC and the DCIs CAPOC accomplish the review recommended on a continuing basis.
JSC_005D	Institute a mechanism to review designation, coordination and integration issues for compartmented access programs and ensure other government elements are advised of such programs affecting their interests.	Implemented through DepSecDef Memorandum, dated 5 Jan 1994 and DCID 3/29, dated 2 Jun 1995. The DoDs SAPOC, DOEs SAPOC and the DCIs CAPOC accomplish the review recommended on a continuing basis.
JSC_006A	Develop a single set of standards for compartmented access.	Implemented through DepSecDef Memorandum, dated 5 Jan 1994 and DCID 3/29, dated 2 Jun 1995. The NISPOM Supplement cites DCIDs as personnel, physical, and technical security standards for all SCI programs. For SAPs, the DoD issued the NISPOM Supplement Overprint recognizing a common set of security standards for each of three sensitivity levels.
JSC_006B	Provide for waivers down from compartmented access security standards when there is no impact upon	Implemented through DepSecDef Memorandum, dated 5 Jan 1994 and DCID 3/29, dated 2 Jun 1995, as well as through SPB Issuance 4-97, Reciprocity of Facilities dated 16 Sept 1997.
JSC_007A	All intelligence reporting within compartmented channels be severely restricted to limit the amount of information that could compromise sources/methods or has exceptional political sensitivity.	Policy issues addressed with the Issuance of DCID 1/7 on 30 Jun 1998. Compliance to be assessed through annual report provided by SPB Staff to the DCI and the DepSecDef on compliance. Staff developing survey tool to support compilation of annual report

Rec #	Recommendation	Implementation / Status
JSC_007B	Intelligence reporting within compartmented channels not related to sources and methods should be released as generally protected information.	Situation improved with the issuance of DCID 1/7 30 Jun 1998. Compliance to be assessed through annual report provided by SPB Staff to the DCI and the DepSecDef on compliance. Staff developing survey tool to support compilation of annual report
JSC_008A	Establish a separate entity to work with special access program managers and combatant commanders to ensure these commanders are aware of compartmented information pertinent to their responsibilities.	Implemented through DepSecDef Memorandum, dated 5 Jan 1994 and DCID 3/29, dated 2 Jun 1995. Continued monitoring required.
JSC_008B	Allow combatant commanders to brief staff members with a need-to-know on compartmented access information.	Implemented through DepSecDef Memorandum, dated 5 Jan 1994 and DCID 3/29, dated 2 Jun 1995. Implementation remains within the management and oversight structures of DoDs SAP Oversight Committee (SAPOC) and the DCIs Controlled Access Program Oversight Committee (CAPOC).
JSC_009A	Rescind the blanket cover status for NRO.	Cover status was rescinded on 25 Apr 1995 by the DNRO.
JSC_009B	Review and limit cover status to covert intelligence or operational missions.	Implemented through DepSecDef Memorandum, dated 5 Jan 1994 and DCID 3/29, dated 2 Jun 1995. Fully implemented under DoDs SAP Oversight Committee (SAPOC) and SAP Coordination Office (SAPCO) and the DCIs Controlled Access Program Oversight Committee (CAPOC).
JSC_009C	Review existing covert contractual requirements to determine those that may be canceled as soon as advantageous.	Implemented through DepSecDef Memorandum, dated 5 Jan 1994 and DCID 3/29, dated 2 Jun 1995. Fully implemented under DoDs SAPOC.
JSC_009D	Develop new policies to limit the use of cover.	Implemented through DepSecDef Memorandum, dated 5 Jan 1994 and DCID 3/29, dated 2 Jun 1995. The CAPOCs annual review of unacknowledged or cover status considers the need for the use of cover.
JSC_010A	The DoD SAPOC should evaluate actual security countermeasures for SAPs and review unacknowledged	Implemented through DepSecDef Memorandum, dated 5 Jan 1994 and DCID 3/29, dated 2 Jun 1995. Countermeasures / security provisions were "standardized" with the issuance of NISPOM Supplement "Overprint".
JSC_010B	Assign security oversight responsibilities for controlled access activities to an independent DoD office outside the special program	Implemented through DepSecDef Memorandum, dated 5 Jan 1994 and DCID 3/29, dated 2 Jun 1995. Security oversight for DoD has been assigned to the ASD/C3I.
JSC_011	With the exception of "GOVIND" and "REL TO," eliminate dissemination and control markings.	Implemented through issuance of DCID 1/7 30 Jun 1998. Compliance to be assessed through annual report provided by SPB Staff to the DCI and the DepSecDef on compliance. Staff developing survey tool to support compilation of annual report
JSC_012	Develop government-wide guidance for sharing classified information with coalition partners and the UN.	The International Security Working Group (ISWG), is working to revive the National Disclosure Policy (NDP). DCID 5/6 issued 30 Jun 1998 is the foundation of the government-wide guidance.
JSC_013	Conduct zero-based review to ensure personnel with need-to-know receive access to SAP info.	Implemented through DepSecDef Memorandum, dated 5 Jan 1994 and DCID 3/29, dated 2 Jun 1995. The DoDs SAPOC, DOEs SAPOC and the DCIs CAPOC accomplish this on a continuing basis.
JSC_014	No individual should sign more than two nondisclosure agreements; one for collateral information and one for compartmented information.	A standardized nondisclosure form has been developed, however the recommendation remains open awaiting the proper technology.
JSC_015A	Classifier should attempt to identify a date or event when information can be declassified.	Sec 1.6(a) of EO 12958 issued 20 Apr 1995 requires this principle be implemented.

Rec #	Recommendation	Implementation / Status
JSC_015B	Aside from limited exemptions, classified information will be declassified after ten years if no date/event is specified.	Sec 1.6(b) of EO 12958 issued 20 Apr 1995 implements this principle but does provide for eight exemption categories.
JSC_015C	For a narrow category of information the 10 year timeline for automatic declassification may be extended to 25 years.	Sec 1.6(c) of EO 12958 issued 20 Apr 97 requires implementation of this principle. ISOO Directive No. 1 provides further specific guidance. Such extensions are exercised by the Original Classification Authority (OCA).
JSC_015D	Specify that a very narrow category of information will be exempt from the 25 year timeline for automatic declassification.	Sec 3.4(b) of EO 12958 issued 20 Apr 1995 requires implementation of this principle. ISOO Directive No. 1 provides further specific guidance. Such extensions are exercised by the agency head, and reported through the ISOO to the President (for approval/reversal).
JSC_016A	Strong oversight is needed from the security executive committee and at the agency level.	Sections 5.3 and 5.4, EO 12958 issued 20 Apr 1995 require both agency and national-level oversight, with ISOO to monitor and report annually to the President on agency programs, and on overall program status.
JSC_016B	ISOO should be part of security executive committee.	ISOO is a member of the Security Policy Forum created by PDD 29 and chairs the Classification Management Committee.
JSC_016C	Agencies need to strengthen oversight and appoint a classification ombudsman.	EO 12958 issued 20 Apr 1995 did not require an ombudsman, but requires agencies to designate an official responsible to direct and administer a program for compliance with the order, to include an ongoing self-inspection program, rating officials on performance of duties under the order.
JSC_017	Establish process to evaluate sensitive but unclassified information within DoD and the IC.	This recommendation has been influenced by recent events. The PCCIP and PDD-63 have caused the Intelligence and DoD communities as well as the rest of government to address the issue of critical information' the aspects of which share a common range of concerns with SBU.
JSC_018	Establish the DCIs counterintelligence center as one-stop shop for CI & security countermeasures threat	PDD-24 issued 3 May 1994, established the National Counterintelligence Center, which was identified as the primary source for threat information. The NACIC is providing foreign CI threat information.
JSC_019	DCIs CI center create a community-wide CI/SCM database for government and industry use.	On 13 Nov 1997, NACIC established a Threat Information collaboration realm on the Extranet for Security Professionals (ESP). Anyone with ESP privileges has access to this realm. The NACIC is currently in the process of populating this realm with unclassified CI/SCM related information and creating links to existing CI/SCM sites. Funding remains an issue with regard to the automated systems.
JSC_020	Clearances should be requested only for personnel who require access to classified information or technology.	Approved by SPB 24 Apr 1995. EO 12968 issued 7 Aug 1995, requires this be implemented.
JSC_021	Fee-for service mechanisms be instituted to fund security requests.	DoD is in the process of implementing fee-for-service for security clearances. The CIA rejects the concept of fee-for-service.
JSC_022	Formal prescreening of contractors be solely performed by the government or an independent contractor hired for that purpose.	NISPOMSUP (Feb 1995), para 2-205, addresses the recommendation in the "Agent of the Government" concept. The Personnel Security Committee of the SPB recommends that prescreening be a self-evaluating process without direct intervention from a third party.
JSC_023	Staff and contract employees should be formally prescreened for a clearance or access only with their knowledge and consent.	The NISPOMSUP adequately addresses the recommendation for contractors. The same procedures should be extended to government
JSC_024A	NISP Personnel Security Questionnaire (PSQ) form be used throughout DoD and the IC.	The recommendation is complete with the adoption of revised Standard Form (SF) 86 in Sept 1995.

Rec #	Recommendation	Implementation / Status
JSC_024B	Develop a standardized prescreening form.	The Personnel Security Committee has made recommendations regarding prescreening but has been unsuccessful with its development. The SF-86 form, appears to be the most complete form available, yet provides no useful information to the applicant regarding their chances for successfully completing security screening process.
JSC_025	DoD and DCI increase investment in automation to improve efficiency	Effective Feb 1999, the DCII and SII computer databases link DoD and OPM systems. Currently, the SAPSSWG is exploring possible data base solutions, to include the DCII, SII, DoDs Joint Clearance and Access Verification System (JCAVS) and a SAP/SCI data base network.
JSC_026A	Investigative standards for TS clearance/SAP access be an SSBI with a scope of 7 years.	The President approved "Investigative Standards" on 25 Mar 1997 in accordance with EO 12968. Although the standards have been adopted by all government agencies, do to financial constraints some agencies are not meeting the standards.
JSC_026B	Investigative standards for Secret clearance be NACI and credit check.	The President approved "Investigative Standards" on 25 Mar 1997 in accordance with EO 12968. DOD implemented 1 Jan 1999.
JSC_027A	Re-investigation for SCA be a SSBI occurring aperiodicaly not less than every 7 years.	The President approved "Investigative Standards" on 25 Mar 1997 in accordance with EO 12968. There is a backlog due to financial constraints at a number of government agencies for re-investigations at both the Secret and Top Secret levels.
JSC_027B	Re-investigation for Secret be a NAC, local agency and credit check conducted on an aperiodic basis not less than once every 10 years.	The President approved "Investigative Standards" on 25 Mar 1997 in accordance with EO 12968. DoD implemented the Secret standards in Jan 1999 but has a significant backlog in Secret re-investigations.
JSC_028	All agencies should have Employee Assistance Programs available.	Approved by the U.S. Security Policy Board on 24 Apr 1995. EO 12968 issued 7 Aug 1995 directs that Employee Assistance Programs be established.
JSC_029A	All investigative and adjudicative organizations begin an orchestrated process improvement program.	The TPDC has completed Investigative Training Standards which are under review by the PSC. Course development should be completed in 1999. The TPDC is developing both a community basic adjudicator course and a Senior Adjudicator Seminar. The seminar is scheduled to run four times annually, beginning in 1999. Core training curriculum is scheduled for completion in Aug 1999.
JSC_029B	Develop standard measurable objectives for adjudications, investigations, and appeals.	The U.S. Security Policy Board developed common adjudicative guidelines and investigative standards to satisfy these requirements and are currently developing training courses to conform to them.
JSC_029C	Interim clearances be granted based on favorable review.	Sec 3.3(c) of EO 12968 issued 7 Aug 1995 implements this recommendation, but the investigation must be no more than five years old.
JSC_029D	Standard interim access process.	The President approved "Investigative Standards" on 25 Mar 1997 in accordance with EO 12968. Access will be granted pending a favorable review of the SF-86.
JSC_030	Adopt common adjudicative criteria.	The President approved "Adjudicative Standards" on 25 Mar 1997.
JSC_031	All DoD adjudicative entities (except NSA) be merged.	Currently under review by DoD/IG and ASD/C3I.
JSC_032A	Any individual who as an existing clearance cannot be re-adjudicated.	Approved by the U.S. Security Policy Board 24 Apr 1995. EO 12968 issued 7 Aug 1995 adopted this recommendation.
JSC_032B	The authorities of program managers to limit access determinations should be limited to does the person have the proper clearance and need-to-know.	Approved by the U.S. Security Policy Board 24 Apr 1995. EO 12968 issued 7 Aug 1995 adopted this recommendation.
JSC_033	Agencies should identify who has conditional clearances or waivers through the use of standard codes.	The SII and DCII databases were linked in Feb 1999. Cases flagged with wavers, exception, etc., are omitted. Phase II is addressing how to accommodate these type coded cases. Programming change to effect the DCII for these cases has been submitted to DSS with a target date for completion of Feb 2000.

Rec #	Recommendation	Implementation / Status
JSC_034A	Clearance procedure safeguards be adopted, but not to include trial type procedures for civilian employees.	EO 12968 issued 7 Aug 1995 incorporates multiple procedural safeguards, but not trial-type hearing.
JSC_034B	All DoD employees facing denial or revocation of a clearance by informed they have a right to counsel.	EO 12968 issued 7 Aug 1995 implements the right to counsel concept.
JSC_034C	Any documents on which a proposed denial or revocation of clearance is based should be available to the DoD civilian employee affected, if privileges and national security allows.	EO 12968 issued 7 Aug 1995 implements the right to documents concept.
JSC_034D	DoD civilian employees facing denial or revocation of a clearance be able to appear before the adjudicative	EO 12968 issued 7 Aug 1995 implements the right to personnel appearance concept.
JSC_034E	DoD civilian employees have the right to appeal an adverse decision.	EO 12968 issued 7 Aug 1995 implements the concept of three-member appeal panel.
JSC_035	With respect to security clearances, military personnel should have the same rights as civilian personnel.	EO 12968 issued 7 Aug 1995 implements appeals procedures that are identical for government civilians and military personnel.
JSC_036A	Screening polygraph should be used by those who already use it, but be limited to CI-scope.	The Forum on 27 Aug 1998 approved a polygraph MOA, that was signed by 12 of the 13 agencies that conduct polygraph programs. The MOA which addresses the 13 JSC recommendations was signed by an agency official, not lower than Director of Security, that maintains a polygraph program.
JSC_036B	Polygraph exams should not serve as a bar to reciprocity.	The Forum on 27 Aug 1998 approved a polygraph MOA, that was signed by 12 of the 13 agencies that conduct polygraph programs. The MOA which addresses the 13 JSC recommendations was signed by an agency official, not lower than Director of Security, that maintains a polygraph program.
JSC_036C	Strict controls of questions and responses must be maintained to limit polygraph abuses.	The Forum on 27 Aug 1998 approved a polygraph MOA, that was signed by 12 of the 13 agencies that conduct polygraph programs. The MOA which addresses the 13 JSC recommendations was signed by an agency official, not lower than Director of Security, that maintains a polygraph program.
JSC_036D	Disqualification should not be based on physiological response alone.	The Forum on 27 Aug 1998 approved a polygraph MOA, that was signed by 12 of the 13 agencies that conduct polygraph programs. The MOA which addresses the 13 JSC recommendations was signed by an agency official, not lower than Director of Security, that maintains a polygraph program.
JSC_037	An independent, external mechanism shall be established to address polygraph complaints.	The Personnel Security Committee of the SPB determined that polygraph complaints were best handled by the individual agencies.
JSC_038	Develop standards to ensure consistency in administration, application and quality control of polys.	The Forum on 27 Aug 1998 approved a polygraph MOA, that was signed by 12 of the 13 agencies that conduct polygraph programs. The MOA which addresses the 13 JSC recommendations was signed by an agency official, not lower than Director of Security, that maintains a polygraph program.
JSC_039A	The CI scope polygraph will be the standard for all contractor personnel.	The Forum on 27 Aug 1998 approved a polygraph MOA, that was signed by 12 of the 13 agencies that conduct polygraph programs. The MOA which addresses the 13 JSC recommendations was signed by an agency official, not lower than Director of Security, that maintains a polygraph program.
JSC_039B	Polygraphs for all contractor personnel working at contractor facilities be conducted under the auspices of a single entity.	Recommendation rejected due to reciprocity of polygraph examinations between polygraph agencies. The Forum on 27 Aug 1998 approved a polygraph MOA, that was signed by 12 of the 13 agencies that conduct polygraph programs. The MOA which addresses the 13 JSC recommendations was signed by an agency official, not lower than Director of Security, that maintains a polygraph program.

Rec #	Recommendation	Implementation / Status
JSC_040	Certify polygraph examiners under the auspices of a single entity.	The Forum on 27 Aug 1998 approved a polygraph MOA, that was signed by 12 of the 13 agencies that conduct polygraph programs. The MOA which addresses the 13 JSC recommendations was signed by an agency official, not lower than Director of Security, that maintains a polygraph program.
JSC_041	Consolidate CIA polygraph school into the DoD polygraph institute.	The CIA school was integrated with the DoD Polygraph Institute in Sept 1995.
JSC_042	Establishment of a robust, centrally funded polygraph research program.	Beginning in FY2000, Intelligence and DoD to sponsor additional Personnel Security research. DoDPI currently has $100K in its yearly budget for polygraph research.
JSC_043	Two-levels of storage protection for all classified material or information.	Recommendation for classified material protection not adopted in EO 12958 issued 20 Apr 1995.
JSC_044	Create a database to record certified Facilities.	The policy for "Reciprocity for Facility Use and Inspection" was approved by President Clinton 16 Sep 1997. Due to the sensitivity of a document that would contain a list of all facilities, the user community opted to develop a list of POCs with knowledge of facilities within their respective organizations. A database of POCs is maintained by the SPB Staff and periodically updated.
JSC_045	No replacement or retrofit of containers and locks currently approved.	This recommendation only affects DoD and the plan for implementation via a prioritization matrix developed within DoD and implemented via DoD 5200.1R was accepted by the SPB.
JSC_046	Routine industrial security re-inspections should be eliminated.	The "National Policy on Reciprocity of Use and Inspection of Facilities" approved by President Clinton limits the frequency of inspections.
JSC_047	Eliminate employment of domestic TEMPEST countermeasures except in response to specific threat data.	NSTISSI 7000 issued 29 Nov 1993 implemented requirements that drastically reduced the use of domestic TEMPEST countermeasures for collateral and SCI and greatly reduced its use for SAPs. All requests must be reviewed by a Certified Tempest Technical Authority.
JSC_048A	Eliminate routine domestic Technical Security Countermeasures (TSCM) inspections in favor of increase emphasis overseas.	The "National Policy for Technical Surveillance Countermeasures" approved by President Clinton on 16 Sep 1997, requires that all programs and inspections be risk base managed and threat driven and that the TSCM be authorized by agency head. The policy is implemented through a series of Procedural Guides and overseen by a working group of program managers.
JSC_048B	The government should fund a coordinated TSCM R&D and training program to support overseas inspections and future technology.	To ensure a continued high level of training, the TSCM training activity has been transferred to the NSA/NCS as the executive agent for TSCM training. Funding to further training and more importantly R&D, remains an issue and a long term strategy is under development.
JSC_049	Develop a Central Clearance Verification database to be made available to government and industry.	The SII and DCII databases were successfully linked in Feb 1999.
JSC_050	Abolish government certification of need to know for contractor visits at the collateral level.	The NISPOM implemented the recommendation, with the exception of non-contract-related visits. These visits require government certification of contractor need-to-know. Approved by the U.S. Security Policy Board on 24 Apr 1995.
JSC_051	Develop a uniform badge system for the government's cleared community.	The Facilities Protection Committee through its Facility Access WG has developed a strategy for a common badge concept and an MOA for the creation of a Configuration Control Board to oversee the strategies development. Work is underway to resolve remaining differences in MOA wording.
JSC_052A	Eliminate requirements to internally track/inventory documents.	Safeguarding Directive Sec VI-Information Controls eliminates administrative control measures which may include internal tracking and inventory and periodic inspections of classified documents, except when technical, physical and personnel control measures are insufficient to deter and detect access by unauthorized person. Safeguarding Directive is at the White House pending approval.

Rec #	Recommendation	Implementation / Status
JSC_052B	Contractors will be authorized routine retention of SECRET classified information.	The NISPOM, Chapter 5, Section 7, para 5-702 allows retention of classified material received or generated under a contract for a period of 2 years after contract completion provided the Government Contracting Activity (GCA) does not advise to the contrary.
JSC_053	Eliminate item-by-item document destruction accountability.	Safeguarding Directive Sec VIII-Destruction, states that classified information is to be destroyed in accordance with procedures and methods prescribed by agency heads. Safeguarding Directive is at the White House pending approval.
JSC_054	Revise document transmittal rules.	Safeguarding Directive Sec VII-Transmission, updates document transmittal rules. Safeguarding Directive is at the White House pending approval.
JSC_055A	Integrate OPSEC into the normal security staff structure & incorporate risk management principles into security training programs.	The OPSEC and Risk Management Training Working Groups under the TPDC have implemented a robust community training program.
JSC_055B	Delete OPSEC requirements from contracts except those in response to specific threat and only when authorized by senior management.	The NISP and the NISPOM have standardized the process.
JSC_055C	NSDD 298 be reviewed, revised or rescinded in accordance with new OPSEC requirements.	A review of NSDD-298 by the TPDC resulted in a recommendation to the Forum that revision of the NSDD was unnecessary.
JSC_056	Develop a coordinated FOCI policy.	The International Security Working Group, under the PIC, reviewed the FOCI policy and found it to be fundamentally sound. However, problems were found regarding consistency of policy awareness and implementation. OUSD(Policy) has incorporated FOCI training and awareness within the Defense Systems Management College's program of instruction.
JSC_057_	Review existing data exchange programs to ensure they are in concert with US national security & economic. goals.	A review was conducted by OUSD(A&T), the DEA proponent. A set of principles for administering DEAs has been established by DoD and disseminated to the services and defense agencies pending staffing of a new DoD directive on DEAs.
JSC_058	Provide comprehensive, coordinated threat analysis and intelligence support to facilitate risk management decisions.	An Intelligence Production Requirements Statement for SCM was agreed to in Apr 1997, and will be forwarded to the NSC for issuance.
JSC_059A	Centralize responsibility for coordinating & overseeing all foreign exchange programs.	Responsibility for DoD foreign exchange programs and issues has been centralized within OUSD(Policy).
JSC_059B	Improve/update national disclosure policy process.	There is general agreement with the language needed to update the national disclosure policy. Final clearance of the new language was requested from the State Department in 1997.
JSC_060A	DoD should expand access to the Foreign Disclosure and Technical Information System (FORDTIS) to command and other consumers.	OUSD(Policy) has expanded access to FORDTIS and continues expansion based upon command and other consumer access requests/needs.
JSC_060B	Ensure CI elements cross-check critical systems and technologies against FORDTIS.	A portion of the OUSD(Policy) international security training and awareness program addresses this issue; however, ultimate utility of FORDTIS database is dependent on consistency and accuracy of "user" (data provider) inputs.
JSC_061	Joint investigative service establish fee for service background investigations.	The concept of a Joint Investigative Service was rejected by DoD. DSS adopted a "fee-for-service" concept in FY 99 for DoD and those DSS supports. Other agencies conducting their own investigations will continue their present practice. CIA rejects the concept of fee-for-service for investigations.

Rec #	Recommendation	Implementation / Status
JSC_062	Joint investigative service to perform industrial security services for DoD and the IC.	The concept of a Joint Investigative Service was rejected by DoD.
JSC_063	Joint investigative service be established and draw resources from existing security organizations.	The concept of a Joint Investigative Service was rejected by DoD.
JSC_064	Consolidate AIS policy formulation under the joint executive security committee, and have it oversee development of a coherent policy for DoD and the IC that also could serve the entire government.	Recommendation not implemented. NSD-42, dated 5 Jul 1990, (as limited by section 10.d), created the NSTISSC, a national level body responsible for issuing national security information systems security policy for the entire Government.
JSC_065	Develop an information systems security investment strategy using 5-10% of infrastructure costs.	Not implemented.
JSC_066A	Give high priority to information systems security research and development programs.	NSD-42, 6.a.(4) and 7.c. authorize the Executive Agent and National Manager to conduct, approve, or endorse research and development of techniques and equipment to secure national security systems. NSA, in conjunction with DARPA, is conducting research and long/short-term development of Information Systems Security solutions.
JSC_066B	Assign NSA as the executive agent for both classified and unclassified infosec R&D.	NSD-42 designates NSA as Executive Agent for national security systems. PL 100-235 designates NIST responsible for unclassified systems with NSA in support role to NIST. National Information Assurance Program (NIAP), a partnership between NSA and NIST.
JSC_067	Assign DISA as the executive agent for providing infosec tools and capabilities.	Not implemented, but will be realized at the FBI's National Infrastructure Protection Center in coordination with GSAs Federal Computer Incident Response Capability, NSAs National Security Incident Response Center, Carnegie-Mellon's Computer Emergency Response Team and DOEs Computer Incident Analysis Center.
JSC_068	Establish an information systems security threat and vulnerability database, available to all DoD, IC, and industry.	NSA makes this information available to DoD, IC, and selected industry through its all-source analysis center.
JSC_069	Appoint DISAs ASSIST program as executive agent for emergency response functions.	Although DISAs ASSIST program was not appointed Executive Agent for emergency response functions, the policy and directive issuances that were intended to make this appointment (NSTISSP 5 and NSTISSD 503) were ultimately used to implement the National Security Incident Response Center (NSIRC) at NSA.
JSC_070	Establish an information systems security professional development program.	Under NSD-42, NSTISSC established the Education, Training and Awareness Issue Group to develop INFOSEC training standards and to assist development of an Information Systems Security Masters Degree Program at James Madison University. Also under NSD-42, NSA assisted NIST in developing INFOSEC training standards for use in protecting unclassified sensitive systems.
JSC_071	Create ad hoc panel to develop common approach and budget framework for defining and tracking. security costs.	A comprehensive framework for capturing estimated costs by security functionality was developed. An abridged version of framework is used to capture annual cost estimates for safeguarding classified information IAW EO 12958. ISOO gathers and reports to the President and Congress the costs to safeguard classified information IAW EO 12958.
JSC_072	Endorse joint government and industry strategy for capturing security costs within a new budget and accounting framework for security.	DoD, as Executive Agent for the NISP, receives annual cost estimates from industry for safeguarding classified information IAW EO 12829. These industry estimates are forwarded to ISOO. However, these estimates are developed on a different framework and algorithm than that used for collecting government security cost estimates IAW EO 12958.

Rec #	Recommendation	Implementation / Status
JSC_073	Develop a long-term resource strategy for security.	Not implemented.
JSC_074	Appoint an executive agent for security Training.	The SP Forum appointed the TPDC as Executive Agent on an interim basis in 1995.
JSC_075	Increase emphasis on developing and funding security education courses for management and up-to-date security awareness programs.	Not Implemented. The community has generally decreased funding and support for both security training and security awareness programs.
JSC_076	Establish a national level security policy committee to provide structure and coherence to security policy, practices and procedures.	The President issued PDD-29 on 16 Sept 1994 which provided the authority and guidance for establishing, supporting and staffing the U.S. Security Policy Board structure.