Considerations for Allocating Resources for Information Security[1]

Marshall D. Abrams, Carolyn M. Johnson, Jay J. Kahn, and Susan G. King
{abrams, cjohnson, jkahn, sking}@mitre.org
The MITRE Corporation, 1820 Dolley Madison Blvd., McLean, VA 22102

Abstract: This paper includes a brief survey illustrating the approach to information security (INFOSEC) investment taken by various organizations, as well as guidelines based on Federal Aviation Administration (FAA) management plans to allocate limited funds among proposals for enhancing National Airspace System (NAS) INFOSEC.

1. Introduction

1.1 Background

The National Airspace System (NAS) of the Federal Aviation Administration (FAA) is being modernized; its increasing use of open systems (publicly available systems) and commercial off-the-shelf (COTS) equipment and software will speed system implementation and lower costs. However, these products, as well as the trend toward more integration among FAA systems, especially among NAS systems, will increase vulnerability to damage, abuse, and system unavailability. While heightened attention to vulnerabilities and evolving threats implies an increasing need for additional information security (INFOSEC), the available funding for protecting the nation's critical infrastructure, including the NAS, has not been increased commensurately.

The FAA's NAS Information Security (NIS) Group tasked the Center for Advanced Aviation System Development (CAASD) of The MITRE Corporation to develop guidelines on how to allocate resources among the programs comprising the NAS to enhance NAS INFOSEC most efficiently. This paper is based on those guidelines.

 This paper is based on work sponsored by the Federal Aviation Administration NAS Information Security (NIS) Group under contract number DTFA01-93-C-00001.

Part of the challenge of developing such an allocation process is that the resources to be allocated and protected include non-monetary values (e.g., lives, reputations, delays) as well as money. One can place a dollar value on compensation for an hour of delay, a damaged reputation (individual, organizational, or corporate), or the loss of a human life. However, such loss or damage should not be considered as involving *only* money. Another consideration is that the costs resulting from inadequate INFOSEC may be incurred by third parties; inadequate NAS INFOSEC can affect the FAA, the airlines, and the flying public.

1.2 Purpose and Scope

This document presents resource allocation guidelines for program INFOSEC. It focuses primarily on the short-term challenge of funding the enhancement of INFOSEC capabilities in the existing and evolving system of systems that comprise the program. It also addresses some operational and longer term resource allocation issues.

As always, management decisions must be made with incomplete data and limited resources. The guidelines herein provide a basis for making the required decisions.

There are no generally accepted formulas for allocating INFOSEC funds. This lack of consensus can be related to one of the major INFOSEC management questions: "How much security is enough?" Unfortunately, a qualitative measure (i.e., a metric) of the security of an information system (or system of systems) is no more within the current state-of-the-art technology than one for a person's health (e.g., resistance to disease). Therefore, no totally quantitative, objective way to make the perfect allocation of resources has been identified; the goal is to allocate the available funds in a reasonable way, based on objectively supportable assumptions.

Certainly, proposals for added or enhanced procedural or technical safeguards should be based on risk assessments for each system in question or for the entire agency. However, the inherently qualitative nature of these assessment results is not as useful for supporting investment decisions throughout the agency as might be wished.

This paper includes a review of the state-of-the-art of approaches to INFOSEC resource allocations that are used by various organizations, recommended INFOSEC resource allocation guidelines, and a set of recommendations for INFOSEC resource allocations.

2. Review of State-of-the-Art INFOSEC Resource Allocations

The authors conducted a review of the state-of-the-art of making INFOSEC resource allocation decisions, based on discussions with representatives from various organizations, and a literature search. The review included the following sources:

- Conversations with individuals who have direct responsibility for INFOSEC at four Federal Agencies, one international financial organization, and The MITRE Corporation
- Conversations with representatives of the General Accounting Office (GAO) about their case studies of INFOSEC in eight non-federal organizations and their observations on Federal Agency resource allocation practices. [6]

- A status report from an INFOSEC cost-estimating project currently in progress by the Big Ten Universities
- Survey results documented in the *1996 Information Systems Security Survey* [3] conducted by WarRoom Research, LLC., in cooperation with the United States (U. S.) Senate Permanent Subcommittee on Investigations.
- The experience of The MITRE Corporation's INFOSEC staff.

The general findings from this review are:

- Quantitative data is not readily available on most aspects of INFOSEC. Even organizations that deal with INFOSEC for monetary items are uncomfortable with the quality of their figures on expected loss and monetary risk.
- Most organizations use an approach to making decisions about INFOSEC capabilities that relies on managerial judgment, based on experience and the best available data.
- The amount of money spent on INFOSEC is not easy to determine. Some reasons are:
  - Organizations in the early phases of developing INFOSEC policies and procedures may not have progressed enough to estimate spending.
  - Organizations further along the INFOSEC development process have included their INFOSEC requirements in the overall requirements of information system projects, so their INFOSEC costs do not appear as identifiable line items.
- There are no general guidelines for determining the percentage of money to spend on risk prevention versus detection versus mitigation. Allocations are often closely tied to an organization's mission; these allocations are frequently situation specific and are often made by and at a low level in the organization's structure.
- System planners agree that it is more cost effective to include resources for INFOSEC mechanisms early in the system development process than to fund their addition once the system is operational.
- Funding decisions focused on newly identified information system threats are often made on an ongoing basis when threats are identified and evaluated. Some organizations have an explicit reserve for funding unplanned risk management projects.
- Some attempts are being made to estimate the costs incurred as a result of INFOSEC incidents. Of 205 respondents to a WarRoom survey question on cost per successful intrusion by outsiders, 27 percent estimated the cost per successful intrusion at between $50,000 and $500,000, 15 percent estimated it at $500,000 to $1 million, and almost 18 percent estimated the cost at over $1 million.

3. INFOSEC Resource Allocation Guidelines

This section documents an INFOSEC resource allocation decision approach in terms of selected relevant factors (Section 3.1) and an analysis process (Section 3.2).

3.1 Relevant Factors

Resource allocation decisions should depend on tradeoffs among several factors within the framework of the overall program INFOSEC goals. Information on most of these factors, to the extent they are known or can be estimated, should be included in each resource allocation proposal and its supporting analysis. These factors are:

- Clear understanding of INFOSEC objectives
- Existence of an INFOSEC plan
- Nature of proposed resource allocations
- The justification of the proposed resource allocations
- System criticality
- Benefits of proposed action and risks of inaction
- System life-cycle phase
- INFOSEC life-cycle phase
- Level of implementation
- Degree of INFOSEC already in place
- Resources required
- Effectiveness of previous related INFOSEC resource allocations
- Shared costs

A brief definition and discussion of each of these factors is provided below. Within the context of the program INFOSEC policy goals, resource allocation decisions should depend on the interplay of these factors for each proposed allocation.

Without *clear INFOSEC objectives*, it is not possible to determine how much security is required in the near term, and how these desired protections advance the overall INFOSEC objectives (i.e., clear bearings and specific objectives).

If there is no *security plan* for the system or systems in question, the most important allocation that should be designated is for the development of such a plan. In its absence, INFOSEC resource allocations are likely to be less effective, ad hoc, or fragmentary, and therefore less effective.

The *nature of the proposed investment* includes descriptions of all proposed activities. In the context of the relevant INFOSEC policy, one should take into account whether the proposed focus is the prevention of, detection of, or recovery from an intrusion or other INFOSEC failure. In theory, preference should be given to *preventing* INFOSEC failures; however, prevention may be prohibitively expensive. For that reason, and because prevention is unlikely to be perfect, a balance among these foci should be sought.

The proposed resource allocation should, preferably, be *justified* by a risk assessment of the system or set of systems to which the allocation is to be applied.

System criticality is the degree to which the loss or degradation of the system may have a negative effect on the agency's mission. In this context, degradation may include denial-of-

service, unauthorized release of sensitive information, or modification of system information to incorrect values. In general, precedence should be given to improving the INFOSEC status of the more critical systems.

The *benefits of the proposed action* include all advantages that will result when risks are decreased or eliminated when the proposed action is taken. The *risks of inaction* include all adverse effects that may occur from not making the proposed investment. If, for example, the proposed investment is intended to decrease the chance that a specified vulnerability will be exploited, the corresponding adverse effect is that the consequences resulting from exploitation will remain the same or increase. In general, preference should be given to decreasing those risks considered most serious.

The *system life cycle phase* covers whether the system for which INFOSEC enhancement is proposed, planned, in development, or operational. In general, preference should be given to making INFOSEC resource allocations as early in a system life cycle as possible, thus reducing the life cycle cost.

The *INFOSEC life cycle phase* indicates whether a proposed investment is for the documentation of a system's existing INFOSEC plans, status, or procedures, for the implementation of improved INFOSEC-related procedures, or for the addition or enhancement of technical countermeasures. Planning for INFOSEC should generally precede the implementation of INFOSEC procedures and technical countermeasures.

The *level of implementation* to which a proposed INFOSEC investment applies may be an individual program or system, a group or category of systems, or the entire agency. It may apply to many facilities, or to a single region or site. As a general proposition, it is more advantageous to fund the broadest proposals. Proposals affecting the program should thus be given priority over program or site specific proposals.

The *degree of INFOSEC already in place* includes whether any INFOSEC countermeasures have already been implemented and their perceived effectiveness. Strengthening an already strong system that is connected to a weaker one may not increase overall INFOSEC.

The *resources required* should include both money and other resources, such as staff time. If the proposed resource allocation will include a continuing resource need, that factor should also be explicitly taken into account.

The *effectiveness of previous related INFOSEC resource allocations* may indicate whether additional investments are likely to prove fruitful. If past investments of the same sort or for the same program are considered to have been ineffective, extra attention may be needed to determine why previous efforts failed and why the proposed investment is expected to produce better results.

Shared costs are associated with the near-term issue that resources must be allocated for security but it is often impossible to identify what portion of the cost is attributable to security. For example, if a wall is required to support a building, what portion should be attributed to security if it is a brick wall instead of a wooden one?

3.2 Analysis Process

The analysis process described here focuses on investing the available monetary resources for the short-term challenge of enhancing INFOSEC through fiscal year (FY) 2000. It has the following requirements:

- Recognize that the information systems environment is not and cannot be made risk free, and that all new risks cannot be anticipated.
- Include the appropriate stakeholders.
- Provide a consistent and systematic evaluation of systems and their corresponding INFOSEC requirements and capabilities.
- Perform analyses without the amount of quantitative data one might like to have.
- Rely on managerial judgment in conjunction with the best available data.
- Respond quickly.
- Allocate resources to respond to unanticipated threats that present new risks to some or all of the program.
- Build in a learning component to improve INFOSEC policies and investment practices for the long term.

The participants in the analysis process should include a core team[2] plus appropriate representatives from the systems and areas affected by each INFOSEC proposal. This team should have organizational visibility, and be at a level that makes formal recommendations to those making funding decisions.

The evaluation of INFOSEC proposals must be based on current, written INFOSEC policies and goals, at least at some basic level, to ensure that key cost considerations are known for all investment proposals.

The system and proposal descriptions should be documented in a consistent format to facilitate the analysis process.

The actual analysis process consists of evaluating the available data, both qualitative and quantitative, and developing a consensus on the acceptable levels of risk in each instance and on how much it is worth to reach those risk levels. In effect, the funding decisions that are made constitute a set of management decisions about the existing vs. acceptable levels of risk in the program and its constituent systems.

The process has two parts: start-up activities and analysis activities. Each part is described below, and their key points are illustrated in Figure 1.

---

2 The core team should include representatives from the agency's central INFOSEC group, sub-area specialists, and representative(s) from the budget and acquisition areas.

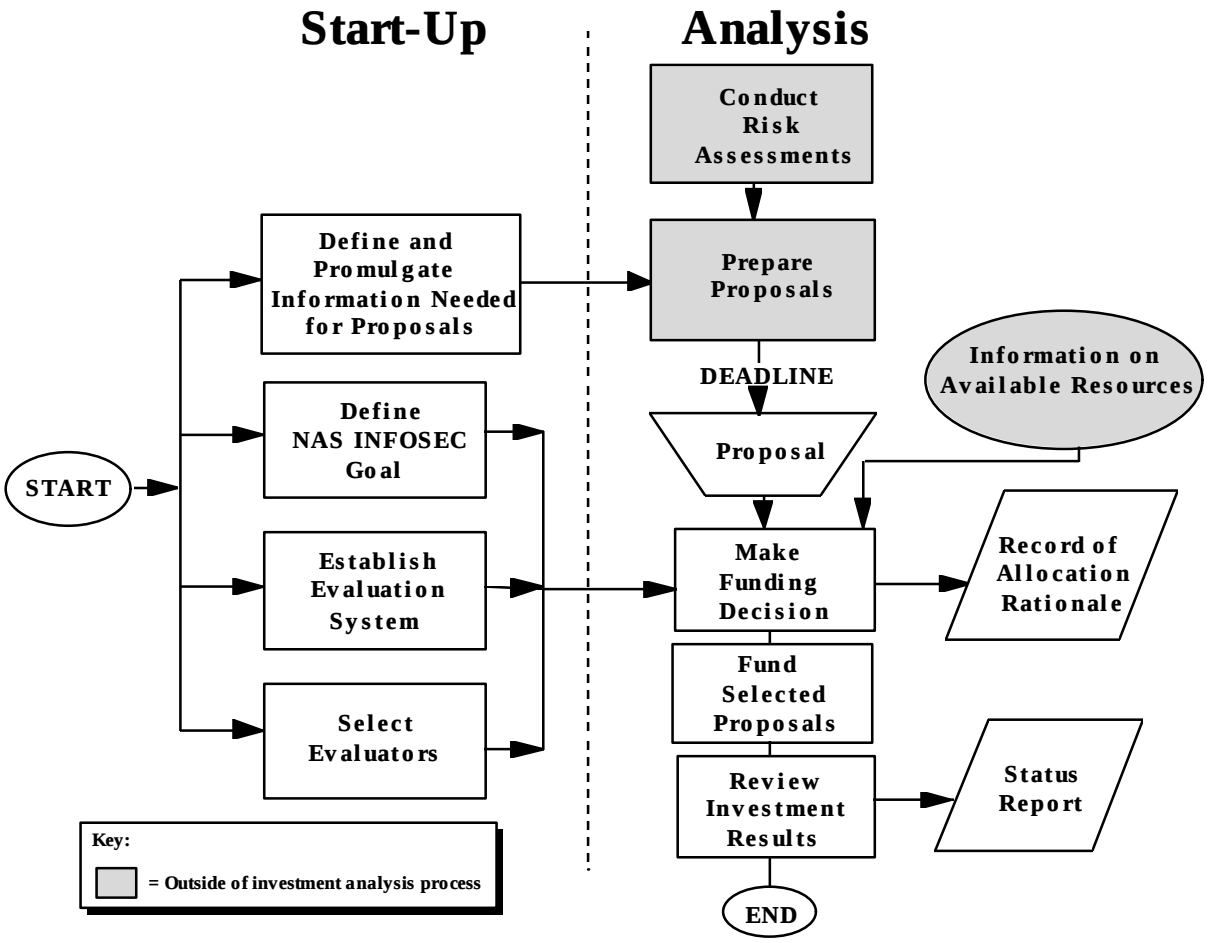

Figure 1. A Short-Term Resource Allocation Process

3.2.1 Start-up Activities

- Select the core resource allocation team participants for the analysis process.
- Prepare the core team charter and have it approved.
- Identify and document up-to-date INFOSEC goals and objectives.
- Establish a rating system. It should be appropriate to the level needed to make recommendations for funding; a straightforward system of high, medium, or low may be sufficient. Section 4: Automated Information Categories and Sensitivities/Criticality Levels of [5] provides an example.
- Identify and document the set of key considerations that will be applied to all proposals. Given the short-term nature of this effort, it may be more effective to focus on a smaller set of what is most important (based on the program INFOSEC policies and goals) than to try to consider every possible aspect. It may be useful to develop a worksheet to record

the outcome of the evaluation of each proposal in relation to the policies and key considerations.

- Define the content and format of the information that should be included in each investment proposal; disseminate these requirements as appropriate.
- Establish a deadline for the proposals.
- Decide on a reserve to set aside for contingency funding.

3.2.2 Analysis Process

- Evaluate each proposal based on the current INFOSEC policies and goals as well as the relevant key considerations.
- If quantitative data are available, and if there is a sufficient degree of confidence in those data, they should be used as appropriate. In the absence of quantitative data, qualitative analyses must be made. In either case, the core team may wish to supplement its program knowledge with relevant technical expertise. For system dependency and interdependency issues, the resource allocation team may include presentations from the organization developing the program architecture.
- Define what it means for each system to be secure.
- Consider the acceptable level of risk. The NASA *Automated Information Security Handbook* [5] provides a good example of how this is done in another Federal agency.
- Consider carefully where a proposal fits into the total effort to enhance program INFOSEC. In particular, ensure that the basics of planning and setting objectives have been completed or are included in the proposal itself. In addition, as set forth in the acquisition system, ensure that non-material efforts, such as the enforcement of existing policies, procedural changes, etc., have been or will be made before investing in new products or tools.
- Record the outcome of the evaluation and analysis in a standard format.
- The cost considerations listed in Section 3.2 indicate areas where preferences should be given for funding. These preferences should be taken into account for making funding recommendations.
- Develop a consensus on the rating of the investment proposal using the rating system developed earlier.
- When all proposals have been rated, evaluate their costs against the available resources.
- Decide whether to fund, partly fund, or not fund each proposal. It is important to avoid the trap of feeling that there must be an INFOSEC investment for every system.
- Use a standard documentation format to record each INFOSEC proposal, the resource allocation decision, and the reasoning and tradeoffs related to that decision.

There is a cost, both in time and money, of performing a lengthy, comprehensive analysis for any investment decision. In the case of risk management investment decisions, where quantitative data often are not readily available (or not available at all), systems are evolving, and new risks are emerging, it is important not to allow the process to jeopardize the security and safety of the program by taking too long to make a funding decision.

4. Agency INFOSEC Resource Allocation Recommendations

This section presents a set of recommended security investments in priority order.

4.1 Short-Term INFOSEC Resource Allocations

Short-term recommendations are addressed here before long-term ones because short-term solutions are generally cheaper and can be implemented quicker. In practice, there will probably be some parallels between short-term and long-term activities: some long-term actions will be started before all short-term actions are completed.

As was previously noted, proposals that are agency-wide in impact should be given priority over proposals that only affect individual programs. However, if the exploitation of a single program's vulnerabilities has a reasonable probability of inflicting significant damage on others, program-specific proposals to deal with such vulnerabilities should be given higher priority.

Additionally, proposals that involve low-cost investments and will have significant impact are given priority over more expensive solutions. Lastly, proposals that are relatively simple are given priority over more complex solutions.

4.1.1 Recommendation #1: Fund the Documentation of the Program Security Objectives

Because there is no such condition as "absolute security," it is incumbent on management to determine INFOSEC goals and objectives, as well as some measures of success. This management concern is often articulated by asking the question, "What does it mean for this system to be secure"?

The costs involved in answering this question should be minimal since the answer does not require engineering and technical analysis. Defining objectives is independent of determining the means for accomplishing them or even determining if these objectives can be met. Defining objectives is a managerial issue; defining means is an engineering issue.

For most agencies, this analysis is a multi-tiered activity. The question can be applied at various levels. There will be an agency-level answer as well as several program-level answers. The NIS Group has addressed this question for the NAS; a draft action plan detailing INFOSEC objectives was published in 1997 [2].

At the program level, each integrated product team (IPT) should document the security objectives for its program(s). This documentation will require minimal resources for most programs.

4.1.2 Recommendation #2: Fund Security Awareness Training

The most cost-effective method for dealing with the security of heterogeneous systems existing at various phases in their life cycle is to develop an educated, security-aware user and manager community. Educated users and managers can prevent the allocation of security resources to unwarranted security solutions that might appear justified to less knowledgeable observers.

Investments in increased security awareness provide dividends by helping ensure that security policies and procedures are followed and that they reflect a system-wide consensus. In summary, security awareness is a low-cost activity with a relatively high return on investment.

4.1.3 Recommendation #3: Fund Virus Protection Programs, Security Gateways, and Other Low-Cost Enterprise-Wide Capabilities

Some forms of security protection can be acquired for very little cost. Examples of these protections are virus protection programs and security gateways such as system-isolating *firewalls* and *screening routers*. Virus problems are well known; new viruses are identified daily. Fortunately, the implementation of virus protection programs does not represent a significant expense or technical challenge.

Legacy systems are expensive to protect. Expertise may have been lost, the system's documentation may not reflect its current design, a version of a COTS product may no longer be supported by the manufacturer. Upgrades are risky as they may require subtle changes to program interfaces. The associated coding and testing phases are time consuming and error prone. If possible, it is more desirable to isolate a legacy system rather than change it. Security gateways provide a useful, cost-effective means for isolating a legacy system since the implementation of a firewall generally does not require modification of the system it is protecting.

Allocating funds for security gateways from a central INFOSEC group has an additional administrative benefit in that it can limit the number of different models of these systems within the program. Standardization simplifies training, logistics, operational procedures, vendor support, and provides a more seamless security implementation within the Agency.

For a small investment, a honeypot system (one that performs absolutely no real function but appears to an intruder to be a choice target) could be created. Such a systems is designed to create intruder notifications whenever anyone attempts to access it, thereby providing immediate evidence that system intruders exist.

4.1.41 Recommendation #4: Fund Security Through IPTs and as Early as Possible in Each System's Development

Since only the IPTs fully understand their systems, they should have the responsibility and funding to analyze, design, develop, implement, test, and document appropriate security solutions.

As previously noted, security must be considered during all phases of a system's life cycle. However, systems that have considered the security implications of all development activities appear to have a more uniform and consistent security implementation, and to contain fewer security flaws at deployment time. On the other hand, systems that attempted to implement security at a late stage in their development tend to demonstrate incomplete security protections, higher costs, and more flaws during accreditation and deployment. Funding the IPTs places resources with those who are qualified to use them to best advantage.

4.1.52 Recommendation #5: Fund the Development of Trusted Communications Among Agency Security Administrators

It would be ironic if hackers could freely distribute encrypted data about attacking the agency while security administrators lacked a secure method of communicating and transferring incident reports and fixes among themselves.

There are many ways that agency security administrators could establish secure communication channels. The allocation of limited resources for experimentation with writer-to-reader encryption would permit proof-of-concept small-scale demonstrations and prototyping of software encryption and key management within the agency.

In the future, these secure communications channels could also be used for software distribution, problem reporting, intrusion reporting, distribution of security warning notices, and a trustable channel between contractors, vendors, the agency Computer Emergency Response Team (CERT), and other CERTs within the Federal Government.

4.1.63 Recommendation #6: Fund the Formulation of Long-Term Security Solutions

There is often a gap between formulating mid- and long-term objectives and applying short-term solutions. To fill this gap, there is a need to fund inter-program studies, program-wide data analyses, network mapping, penetration tests using one system to verify the security of another, and the performance of program-wide risk analyses. The results of these activities will form the basis of long-term program security planning.

Additionally, this type of activity can be used on a much more limited scale as a means of gathering data for near-term contingency plans. Top-level managers should formulate policies that enhance and encourage inter-program cooperation, security data sharing, and coordinated responses.

4.1.74 Recommendation #7: Develop Reserve Funds to Meet Contingencies

Unexpected INFOSEC contingencies may be expected. A new virus may appear, hackers may attack the system requiring file restoration, or some other security incident may occur. There should be a reserve fund to pay for contingency action. Allocation of resources to a contingency fund is a prudent act.

Also, some programs may require additional funds because the security risks were underestimated whereas others may require additional funds because the proposed risk reduction mechanism was not sufficiently effective or was poorly implemented.

4.2 Long Term INFOSEC Resource Allocations

4.2.1 Recommendation #8: Track the Results of Investments

INFOSEC tends to be dynamic, so security plans are subject to frequent changes. These changes must be managed and assessed.

As the funds are spent, data indicating how effective the investment has been should be collected.

4.2.2 Recommendation #9: Phase Out Separate Facilities and Engineering (F&E) Security Budgets

Although the security engineering community is not fully in agreement, there is an emerging view that allocating money specifically for INFOSEC is inefficient. In this viewpoint, security is either an integral part of a system or it is unnecessary. Attempts to engineer security independently from functional development are less effective than treating security as another system service and, therefore, as just additional system requirements.

Applying this perspective to agency systems, INFOSEC is the responsibility of each IPT and should be treated as part of the comprehensive cost of developing or enhancing any system.

Program-wide INFOSEC resource allocations should be approved as needed. Also, INFOSEC resource allocations should continue to be included in acquisition review, as has been done recently in the FAA's Major Acquisition Review (MAR) cycle.

Acknowledgments

We appreciate the contributions of: Bob Taylor, Federal Reserve Board (Fed), Information Resource Management (IRM) Division, Advanced Technology Group, Tom Judd, International Monetary Fund (IMF), Information Security, Kathy Kimball, University Computer, Network and Information Security Officer, The Pennsylvania State University, Jean Boltz, Government Accounting Office (GAO), Mike Gilmore (GAO), Greg Wilshusen (GAO), Ed Glagola (GAO), and Ronald Beers (GAO), who gave generously of their time and expertise.

List of References

[1] EO 13010, 15 July 1996, Presidential Documents, *Critical Infrastructure Protection,* Washington DC.

[2] *National Airspace System (NAS) Information Security Action Plan* (Coordination Draft), 21 May 1997.

[3] WarRoom Research LLC. "1996 Information Systems Security Survey".

[4] Department of Defense, December 1985, *Department of Defense Trusted Computer System Evaluation Criteria,* DOD 5200.28-STD, Washington DC.

[5] National Aeronautics and Space Administration, June 1993, *Automated Information Security Handbook,* NHB 2410.9A.

[6] General Accounting Office, 1997, *Executive Guide: Information Security Management: Learning from Leading Organizations,* available at http://www.gao.gov/special.pubs/publist.htm, GAO/AIMD-98-68.

[7] Science Applications International Corporation (SAIC), 1997, *Organization and Business Case Model for Information Security*, available at http://www.ncs.gov/n5_hp/Reports/N5Documents.html.