ABSTRACT

Title of Dissertation: **IMPROVING THE QUALITY OF INFORMATION TECHNOLOGY (IT) SECURITY AUDITS FOR FEDERAL AGENCIES**

Ellen Pieklo, Doctor of Management, 2005

Dissertation Directed By: **Dr. David Cohen**
University of Maryland University College (UMUC)

The study examines Government Accountability Office (GAO) IT security audit reports for a two-year period to assess the quality of these reports, addressing three questions. The first question is: do GAO reports provide a high-quality, independent assessment of IT security programs? The second question is: do GAO reports provide federal agencies with sufficient information to correct IT security problems? The third question is: Do GAO reports provide a feedback mechanism to allow another agency to learn from the mistakes of another agency?

Federal agencies are spending over $50 billion per year on information technology and are encouraged to be results driven yet these same agencies are unable to manage and protect the information. In a recent assessment, over half of federal agencies received a score of "C" or "D". In 2004, the average score is still D+. Other reports showed that sensitive data is available on public web sites, fraud has been committed against the government, and federal computer systems are exposed to computer attacks and reached over 1.4 million attacks in a 2003.

This study looked at the GAO reports to determine if the current audit reports provide an effective approach to evaluating IT security environments, using the concepts of validity, reliability, and practicality. Two hundred and six findings were evaluated from these reports. The study concludes that IT security audits do not effectively assess IT security environments. Relative to the three questions, the study found: 1) GAO reports do not provide a high-quality, independent assessment of IT security programs 2) reports do not provide federal agencies with sufficient information to correct IT security problems and 3) GAO reports do not provide a feedback mechanism to allow another agency to learn from the mistakes of another agency.

In addition, the study recommends: 1) federal agencies conduct IT security audits enabling statistical sampling; 2) federal agencies use better research methods; and 3) federal agencies improve the feedback processes. In addition, the study introduces the Ten Step Security Delphi Model, which can be used as a technique to prioritize security weaknesses.

IMPROVING THE QUALITY OF INFORMATION TECHNOLOGY (IT) SECURITY AUDITS FOR FEDERAL AGENCIES

By

Ellen Pieklo

Dissertation submitted to the Faculty of the Graduate School of the

University of Maryland University College

in partial fulfillment of the requirements for the degree of

DOCTOR OF MANAGEMENT

2005

Doctoral Committee:
Dr. David Cohen, Chair
Dr. Carlo Broglio
Dr. Dipak P Pravin
Dr. Claudine SchWeber

Dedication

This dissertation is dedicated to my husband and friend, Dr. Thomas Pieklo. You've encouraged me to follow my dreams and pushed me to catch them.

Acknowledgements

I'd like to acknowledge my dissertation committee, including Dr. David Cohen, Chair, Dr. Carlo Broglio, Dr. Dipak P Pravin, and Dr. Claudine SchWeber. I appreciate of all of the time and effort you've spent with me, reviewing and editing my concepts, helping me to organize my dissertation in the best manner possible, and finally for helping me to see this process through to completion. To all of you, I express my deepest gratitude.

Table of Contents

List of Tables and Figures

Abbreviations & Acronyms

Acronym	Meaning
AICPA	American Institute of Certified Public Accountants
CISSP	Certified Information Security Professional
DC	District of Columbia
DOD	Department of Defense
FBI	Federal Bureau of Investigation
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act
GAO	General Accounting Office
GAO	Government Accountability Office
GISRA	Government Information Security Reform Act
I&A	Identification & Authentication
ID	Identification
IG	Inspector General
IRS	Internal Revenue Service
ISSA	Information Systems Security Auditor
IT	Information Technology
LOU	Limited Official Use
NBST	National Bureau of Standards & Technology
NIST	National Institute of Standards & Technology
NSA	National Security Agency
NT	New Technology
OMB	Office of Management and Budget
OS	Operating System
PMA	President's Management Agenda
SSA	Social Security Administration
TQM	Total Quality Management
UMUC	University of Maryland University College

Chapter 1: Introduction

The federal government has an obligation to protect the information it processes yet computer systems have been and remain at risk of being compromised (Computer Science & Telecommunications Board, 1991). In 2002 and 2003, fourteen of twenty-four federal agencies received grades of C or below and eight agencies failed (Morrison, 2004) in protecting its computer systems, as required by the Federal Information Security Management Act of 2002 (FISMA). In 2004, the average grade was a D+ (Davis, 2005).

What do these grades mean? Security grades are calculated and assigned by the Office of Management and Budget (OMB) and Congress, using the results of independent annual evaluations and Inspector General (IG) audit reports. The scoring is assigned using grades of A through F, allowing managers to easily assess how the agency is performing IT security. So far, the results are not good.

Congressman Adam Putman, Chairman of the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, has been working to explore progress of the E-Government Act of 2002 (Dhar, 2004). Regarding IT security, Representative Putman stated:

> "Today we continue our in-depth review of cyber security issues affecting our nation. Specifically this hearing will focus sharply on the efforts within the Federal Government to secure our own computer networks. Our critical infrastructure, of the cyber kind, must have the same level of protection as our physical security, if we are to be secure, as a Nation, from random hacker intrusions, malicious viruses or worse – serious cyber terrorism. There are several things unique to cyber attacks that make the task of

> preventing them particularly difficult. Cyber attacks can occur from anywhere around the globe: from the caves of Afghanistan to the war fields of Iraq, from the most remote regions of the world or simply right here in our own back yard. The technology used for cyber attacks is readily available and changes continually. And, maybe most dangerous of all, is the failure of many people -- critical to securing these networks and information from attack -- to take the threat seriously, to receive adequate training, and to take steps needed to secure their networks. A serious cyber attack could have serious repercussions throughout the nation both in a physical sense and in very real economic dollars (Putnam, 2003)."

If these low scores are accurate, the American public has no assurance that the federal government is meeting its financial and program responsibilities. Using computer systems with weak security controls may result in monetary damages and a compromise of information for federal agencies. In January 2004, the Wall Street Journal announced that the biggest web problems weren't privacy issues but sloppy security (Gomes, 2004). Gomes learned that web-based applications are often easy to compromise, resulting in a situation in which unauthorized people can access the information processed via the web applications. There is a potential that these systems could be compromised for fraudulent purposes.

Weak security controls have already resulted in the loss of privacy of individuals using the Internet, as identified by the FBI (FBI, 2003). For federal agencies, the compromise of government data could be catastrophic in the areas of confidentiality, integrity, and availability. If the Social Security Administration compromises the social security numbers of the American

public, this could impact the mission; people would lose confidence in the ability of Social Security to protect personal information.

There is also a potential that the federal government might not be able to provide services in the event of crisis situations. In March 2003, the Government Accountability Office (GAO), formerly known as the General Accounting Office, reported that there were over 1.4 million cyber-security attacks launched against the government, up from 489,890 in 2002 (Mark, 2004). According to the National Research Council, federal agencies are unable to manage information under crisis conditions (National Research Council, 2003, p.2). The National Research Council stated that if there is a catastrophic event in the United States, the federal government may not have adequate preparation for alternate operational plans provided by using formal contingency planning. Alternate plans are those plans which allow an agency to resume normal business operations in the event of a disaster. The significance is that if a terrorist event occurred at a government agency, the agency may not be able to provide services to the public, due to inadequate planning. The National Research Council noted that while September 11th had little effect in some areas of the Internet, the true impact is not really known, since the ability to measure harm is limited due to the lack of relevant data (National Research Council, 2003, p.2).

Years after the National Academy of Science suggested federal computer systems were at risk, the federal government still fails to implement effective IT security programs (NAS, 1991). NIST estimated poor software practices cost the economy $59.5 billion (Putman, 2003, December 9). In spite of the increased security risks, the government spends $ 50 billion per year on information technology and is a major partner in electronic commerce (Bush, 2002).

Section 1.1 Relevance

The need to improve the quality of IT security audits is relevant for several reasons. First, the GAO performs the role of an independent auditor for federal agencies. The GAO provides assessments of federal agencies, provides briefings to Congress on security-related issues, and can directly impact new initiatives mandated to federal agencies. In addition, the GAO provides guidance to other federal agencies identifying procedures for conducting audits within individual agencies. The *Federal Information Security Controls Audit Manual* (FISCAM) defines the process used to conduct GAO audits. The GAO recommends federal agencies use this methodology to evaluate the controls of individual federal agencies to assess compliance for integrity, confidentiality, and availability of data (GAO, 1999, preface). As the role model for conducting audits within federal agencies, it is both significant and relevant that the GAO process be examined.

Second, IT security programs are now required to provide measures of performance. Funding may be impacted when programs have poor security. On September 1, 2002, President Bush issued a statement and strategy to Congress to improve management and performance in the federal government (Bush, 2002). President Bush identified five government-wide goals, including: Strategic Management of Human Capital; Competitive Sourcing; Improving Financial Performance; Expanded Electronic Government (E-Government); and Budget and Performance Integration, all dedicated to reforming the government. IT security falls within the scope of E-Government, which is designed to provide better access to government information to the American public and to other agencies.

The President's Management Agenda (PMA) provides a vision for reform guided by three principles: citizen centered, results oriented, and market-based (OMB, 2002). Scores were

defined by the President's Management Council and discussed with experts throughout government and academe, including individual fellows from the National Academy of Public Administration (OMB, 2005). The PMA provides accountability for results.

Using the PMA, measurement of success is accomplished using a stoplight scoring system or a "scorecard," in which green indicates success, yellow indicates mixed results, and red indicates unsatisfactory results (Bush, 2002). This is similar to the security scorecards, where agencies are rated with scores of A through F. While the security scorecard assigns a letter grade, the stoplight uses the colors to show progress.

Using the PMA, agencies must be able to measure the success of their IT security programs and only successful programs will receive funding. In 2003, over one-third of the agencies received a grade of "C" or "D" (Putman, 2004). In 2004, the average grade was an improvement but still D+ (Davis, 2005). This report was published by Tom Davis, of the Government Reform Committee in 2005. Unless agencies can improve IT security programs, IT projects will be at risk of losing funding due to the poor IT security ratings. Managers of federal agencies will need to understand the factors that contribute to successful scores.

Agencies who received good security grades did maintain common characteristics: 1) completed inventories of their critical information technology assets; 2) identified critical infrastructure and systems; 3) implemented strong incident reporting procedures; 4) had tight controls over contractors; and developed strong plans; and 5) milestones for finding and eliminating security weaknesses (Strohm, 2003).

Chapter 2: Research Problem

Recently, the Congress reported that over 1/3 of twenty-four government agencies failed program assessments of their computer security programs and over half of the remaining agencies received grades of "C" or "D" (Putman, 2004). In 2004, over half the agencies had scores of "D" or "F". See page 14, which contains the federal IT security grades, published by Congress.

The grades are calculated from the results of agency audits and independent assessments. What is the impact on the scores if there is no validity to the audits? Assume the audit reports are valid. If an auditor conducted an audit and identified serious problems to management, one could reasonably expect that the agency would attempt to correct the problems, resulting in an improved security score for the following years. This has not been the case. It may be possible that security cannot be easily improved because the audit reports are not clearly understood.

Do audit procedures used by GAO provide an effective assessment of IT security environments within federal agencies (GAO, 1999)? Do these reports contain sufficient information to allow federal agencies to adequately understand, prioritize, and correct the problems? If current audit reports do not provide an accurate assessment, how can the quality of audits improve? As federal agencies enter the world of electronic commerce and continue to spend billions of dollars on information technology, these questions must be answered to ensure the security of these systems is not compromised.

The objectives of this study were to evaluate the quality of GAO reports during a two-year period, as this relates to IT security audits, and to determine if these audits provided an effective assessment of the IT security environment. The study attempts to answer three

questions. The first question is do GAO reports provide a high-quality, independent assessments of IT security programs? The second questions is do the reports provide federal agencies with sufficient information to correct IT security problems? The third question is do GAO reports provide a feedback mechanism to allow another agency to learn from the mistakes of another agency?

Section 2.1 Constraints

The first constraint of the study was that this study used public versions of GAO reports. There are additional reports, identified as Limited Official Use (LOU), which contained more detailed information. This information was not available. While the LOU reports contain more detailed information, the process remained the same. As a result, the constraint had minimal impact. The second constraint was that the study used reports published prior to 2004. Since then, there may have been efforts by the GAO to integrate additional evaluation techniques. For example, NIST published new guidance on integrating the use of metrics to evaluate IT security programs (NIST, 2005). The third constraint of the study was that this study only applies to audits of federal agencies and IT security related audits. The fourth constraint is that cost is not discussed as part of this study. While cost is an important consideration, the focus was on assessing whether GAO reports provide sufficient information to understand IT security problems.

Chapter 3: Literature Review of IT Security Controls

Section 3.1 Historical Perspective

For the past thirty years, computer security controls and requirements have been defined for government agencies. These requirements now include over two-dozen individual security manuals (NSA, 2004; NIST, 2005). The National Computer Security Center (NCSC) has been a key agency in authoring many of the security requirements and has published over twenty-four documents designed to protect computing systems and the information contained on these systems. Some of the subject areas published by NCSC include: protecting operating systems; protecting networks; validating application security; and removing residual data (NSA, 2004). During this same period, the National Institute of Standards & Technology (NIST), formerly known as the National Bureau of Standards and Technology (NBST) also published IT security related guidance, in the form of Federal Information Processing Standards (FIPS). These documents supplemented the National Security Agency requirements and provided implementation guidance. These documents are provided on the FISMA Implementation Site, one of the NIST web pages (NIST, 2004).

Appendix 1 contains a comprehensive list of IT security-related requirements, as these have evolved over time (NIST, 2004). Most recently, the federal government published the Federal Information Security Management Act, containing new security reporting requirements.

Though the federal government has been mandated to implement these security requirements, federal agencies are unable to effectively implement and manage their IT security programs. This is a serious management problem. Management is now accountable, due to the introduction of the President's Management Agenda (OMB, 2003).

Section 3.2 Federal Agencies Are Not Compliant with IT Security Standards

Historically, federal agencies are not complying with IT security requirements. The Computer Security Act of 1987 required federal agencies to report security plans for their computer systems, yet in 1991 the National Academy of Science wrote a book describing the poor security state of federal computing systems (NAS, 1991).

Since 1997, the GAO has also identified the poor security of information systems as a high-risk issue (GAO, 2004). Most recently, the Federal Information Security Management Act (FISMA) of 2002 provided "new" requirements for IT security. FISMA instituted new reporting requirements but merely mandated already existing guidelines (NIST, 2004). After two reporting periods, Congress identified IT security as a major concern (Putman, 2003, December 9).

In 2003, the GAO reported federal agencies did not understand their responsibilities and the GAO found the same problems identified earlier in the mid 1980s (GAO, 2004). Federal agencies continue to spend millions of dollars to correct security, with little success. According to the most recent scorecards, only two agencies of twenty-two received scores of "A" and 66% received scores of "D" and "F". The significance is that federal agencies may not adequately protect the information it processes. As a result, private information of individuals may be compromised.

In the testimony before the subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Congressman Putman identified serious deficiencies, within the federal agencies' IT security programs including:

a) "Agencies report the same security weaknesses year after year, such as lack of system level security plans and certifications and accreditations;

b) Some Inspector Generals (IG)s and Chief Information Officer (CIO)s -- from within the same agencies -- have vastly different views of the state of the agency's security programs;

c) Many agencies are not adequately prioritizing their IT investments and are seeking funding to develop new systems while significant weaknesses exist in their legacy systems;

d) Not all agencies are reviewing all programs and systems every year as required by Government Information Security Reform Act (GISRA);

e) More agency program officials must engage and be held accountable for ensuring that the systems that support their programs and operations are secure. The old thinking of IT security as the responsibility of a single agency official or the agency's IT security office is out of date, contrary to law and policy, and significantly endangers the ability of agencies to safeguard their IT investments" (Putman, 2003, December 9).

The significance of Putman's findings is that the federal agencies are not able to provide improved security but continue to seek additional funding for new systems, without first correcting the inherent IT security problems.

Security for federal IT systems is not improving. Putman noted that even as President Bush established a Homeland Security organization to provide better security, the agency most responsible for protecting terrorist-related information did not receive passing grades in protecting its own sensitive information (Putman, 2003, December 9).

Section 3.3 Effects of Poor IT Security

IT security is an integral component of a comprehensive enterprise security program. While IT security protects the technology resources, security is only as strong as the weakest link. If there is a failing in any of the fields of security, the entire security posture is impacted.

In many cases, federal agencies are still not aware of the roles and responsibilities for implementing security controls. Many of the government's weak controls have been cited, since the terrorist events of 9/11/01. As the government probed into some of the problems related to 9/11, Congress learned that many agencies posted information on web sites that provided access to security maps of key facilities, such as diagrams of sensitive security facilities. In addition, communication issues were identified, where management from one federal agency did not provide the information, as necessary, to another federal agency. The effects of poor IT security within the federal government cost our economy millions of dollars each year.

In May 2002, the GAO conducted a study of the Department of Education and two Navy units (GAO, May 2002) and found weak security controls allowing credit card holders to make fraudulent, improper, abusive, and questionable purchases. In this report, the GAO reviewed five months of credit card purchases. 37% of the purchases were not approved by the appropriate official, when purchases equaled $1.5 million. On occasion, computers were purchased but never logged into files for recordkeeping (GAO, May 2002). In addition, where credit card purchases were authorized, one official was responsible for the review of 1,153 cardholders.

Within the Department of Agriculture, there were 50,000 computer generated alerts but only 29,600 were reviewed. By reviewing security reports, management is able to be alerted to situations that may require further attention. The lack of review causes a potential for fraud and

abuse. In all of these cases, the government agencies are responsible for monitoring the use of computer records but not able to effectively accomplish the necessary reviews.

The Social Security Administration's Supplemental Security Income (SSI) program was designated as a high risk program in 1997, partially because of the susceptibility to computer fraud (GAO, May, 2002). The 2002 report indicated that the programs were under revision but due to the early stages of the program, the high risk was still present. The current efforts include recovering $61 million in SSI overpayments made during the last year.

Although the Social Security agency is using computer matching to recover lost funds, the organization still plans to use the Internet to provide telephone and electronic access services to integrate a paperless process. The significance is that the Social Security Administration is moving forward with technological improvements without fully correcting ongoing IT and security related issues.

The GAO has also noted that social security numbers were compromised and false identities were obtained by the terrorists who caused the national disaster on September 11, 2001.

In yet another report, the GAO found Department of Education employees bypassed controls on the computer system designed to prevent duplicate payments. There were $8.9 million identified as potential improper payments (GAO, March, 2002). Similar computer weaknesses and controls were identified with other federal agencies (GAO, January 2002; GAO, May 2002).

Since 1999, the General Accounting Office has faulted the Environmental Protection Agency; Department of Defense; National Aeronautics and Space Organization; and Department

of Veterans Affairs with having security related weaknesses on computing systems, often placing the government at risk to hackers and terrorists (GAO, 2002).

In 2003, when Congress first surveyed the IT security of government agencies, the rating of D was the overall grade for the protection of information for twenty-four government agencies (Dorobek, 2003). As federal agencies struggled with protecting their computer systems, some agencies compounded the problem with their own inadvertent disclosure of sensitive information. Prior to September 11, 2001, government agencies stored a vast amount of sensitive information on the Internet unintentionally exposing the country to harmful risks.

In 2001, federal agencies were chastised for providing functionality, where security controls may have been compromised. Most recently, the White House had to educate federal agencies to remove sensitive data from web sites, including information on weapons of mass destruction (Sammon, 2002). While the need for stronger security controls has already been identified, the poor government score cards indicate the solution is not at hand. As security becomes a higher priority within the United States, the need to protect information becomes critical to all federal agencies.

Financial loss is a key concern to government agencies. The Computer Security Institute indicated that 90% of the companies and federal agencies surveyed detected a breach of security and of these, 74% indicated there were financial losses. Losses were quantified at over $265 million dollars (Desmond, 2000).

Section 3.4 Security Is Not Improving

According to the newest computer security grades assigned to the government, of twenty-four agencies evaluated in 2002, over 50% received a grade of “F”. While there was a significant improvement in 2003, 1/3 of the agencies still scored a grade of an “F” and only two agencies

achieved a score of "A": the Nuclear Regulatory Commission and the National Science Foundation. The research indicates that good federal government computer security programs are the exception rather than the rule. Table 1: *Federal IT Security Grades* provides the recent grades assigned to federal agencies for their IT Security Programs (Putman, 2004 & Davis, 2005). The 2004 report card was released by Representative Tom Davis, of the Government Reform Committee. Though the scorecard is used, Putman has questioned the validity of the scorecard because five of twenty-four agencies did not conduct the required inventory of critical assets (Saita, 2003).

Table 1 - Federal IT Security Grades, As Published by Congress

Agency	2002 Grade	2003 Grade	2004 Grade
Nuclear Regulatory Commission	C	A	B+
National Science Foundation	D-	A-	C+
Social Security Administration	B-	B+	B
Department of Labor	C+	B	B-
Department of Education	D	C+	C
Department of Veterans Affairs	F	C	F
Environmental Protection Agency	D-	C	B
Department of Commerce	D+	C-	F
Small Business Administration	F	C-	D-
Agency for International Development	F	C-	A+
Department of Transportation	F	D+	A-
Department of Defense	F	D	D
General Services Administration	D	D	C+
Department of the Treasury	F	D	D+
Office of Personnel Management	F	D-	C-
National Aeronautics and Space Administration	D+	D-	D
Department of Energy	F	F	F
Department of Justice	F	F	B-
Department of Health and Human Services	D-	F	F
Department of the Interior	F	F	C+
Department of Agriculture	F	F	F
Department of Housing and Urban Development	F	F	F
Department of State	F	F	D

Section 3.5 Federal Agencies Must Get to "Green"

The President's Management Agenda (PMA) is already working to improve management in the federal government and move all agencies to "green" (OMB, 2002). As previously discussed, the PMA uses a scorecard system to define measures for success (OMB, 2004, August 24). Success is measured, relative to cost, schedule, and performance. To achieve green, the agency's performance cannot vary from the goals by more than 10%. To achieve yellow, the performance cannot vary by more than 30%. As agencies are pressed to substantiate program successes, agencies will need to have better tools and techniques to document and validate performance measures.

There are serious consequences for federal agencies when IT security fails. First, poor security practices lead to fraud, waste, and abuse. Second, IT systems at placed at risk of exploitation. Third, federal agencies may not be capable of carrying out the mission. Fourth, funding for the government programs may be lost where security controls cannot be effectively measured and validated.

Section 3.6 Research Identifies a Need for Better Management Tools

As knowledge and technology continue to grow, more and more information will be stored on government computer systems. For IT security managers, this increased workload will be significant. For example, IT security personnel use computer auditing techniques for two important security functions: surveillance and monitoring (O'Reilly & Associates, 1992, p. 129). Auditing of computer systems allows events to be captured including: the date and time of a user action, success or failure of an action, user who performed the action and the action performed. In a federal agency, until recently, users did not have the capability to interact with government agencies via web-based applications. With the introduction of new technologies, the number of

users accessing a federal computer system could reach into the thousands each day. IT security management is tasked with reviewing these audit logs to determine if malicious activity has taken place, yet to accomplish this task manually would be virtually impossible. Likewise, if configuration settings are to be audited to ensure security controls remain persistent, the volume of audit logs will grow exponentially. The management challenge is to introduce effective and automated tools to facilitate IT security tasks. To accomplish this, federal managers require better management and decision-making tools and techniques to identify the problems and to manage the processes for IT security programs.

Risk assessments provide one management tool, allowing IT security managers to assess the threats of their computer systems and to determine where threats are most vulnerable. This is accomplished by identifying potential threats to the system and associating the threat with a likelihood of occurrence, and with the cost of replacing the resource being protected. Once mapped, management can ensure the most vulnerable threats are protected by implementing cost effective countermeasures. Whenever security concepts are integrated into an organization, the need to improve security must be balanced with the cost of the product against the risk of the threat (O'Reilly, 1991, p.91-93). Risk assessments allow security measures to be implemented, relative to cost, threat, and likelihood of occurrence. By using risk management practices, agencies can implement security controls, which are cost effective, based upon the potential of a threat to occur (Phleeger, 1989, p.457-458).

There are variations of implementing risk management practices. Another option is to identify threats and to rank these in order of importance and impact to the organization, allowing for the threats to be minimized on the basis of loss, embarrassment, and probability of occurrence (Newman, 2003, p.248-249). Prioritization of risk-based approaches is another

decision-making practice. The transportation sector, Department of Transportation, has been faced with assessing a multitude of disasters and assigning risk values to these disasters. The agency is using a prioritized, risk-based approach to provide practical and affordable solutions (Volpe, 2003). In all of these instances, managers at federal agencies continue to be faced with the task of implementing security controls, in a cost effective manner, using better management processes.

Federal agencies are already using risk-based and cost-based models and concepts of prioritizations in the field of IT security. Both government and industry are concerned with utilizing automated tools to provide better IT security practices. When conducting a search on audit sampling tools on the Internet, 143,000 web sites match the criteria.

Though there are many provisions to manage security, federal agencies continue to fail to meet their responsibilities. As Putman's testimony noted, many federal agencies have poor IT security, with the current average identified as D+ (Yasmin, 2005). New research must be conducted to determine how to best identify and correct security concerns using risk-based concepts. Auditing is one program area in which federal managers could benefit from the availability of better management tools. Agencies must work to obtain more value from audit reports, allowing information to be categorized, analyzed, and managed. By providing better analysis, management can make better determinations on problem resolution.

Additional value from an audit can be obtained from one of the following: 1) better understanding the nature of an observation and 2) understanding the severity of an observation. This can be accomplished using statistical sampling methods. Sampling is not always used for conducting IT security audits. GAO has determined these techniques are not necessary (GAO, 2004).

Section 3.7 Potential Causes of Poor IT Security

There are many potential causes of poor IT security. These include: lack of management support; confusing and complex security requirements; lack of subject matter experts; competing resources between security and functionality; and the technical challenges, i.e. Enterprise Security Issues.

GAO personnel contend the lack of management support is one of the key causes of IT security problems (GAO, 2004, November 29). When management places a high value on program areas, employees will tend to use the same priorities in accomplishing their own workload. This is exactly what Deming found when implementing quality programs within organizations. Top management involvement is required, including clear plans for quality leadership, to implement successful programs (Gabor, 1990, p.270).

Earnst & Young's Global Information Security Survey, released to over 1,233 businesses found that despite an increase in regulations, only 30% of the boards of directors receive updates on security issues. In addition, the survey stated that management does not recognize the importance of information security (Thomas, 2004). Until management addresses security issues, there will be no efforts to prioritize or to correct these issues.

Currently, federal agencies are faced with the challenge of implementing a multitude of security requirements. FISMA identifies over thirty-four documents, as part of the FISMA implementation efforts (NIST, 2005). Appendix 1: Federal IT Security Requirements contains a list of security requirements, sorted by date of publication.

Each of these security documents is complex. As an example, Microsoft Corporation worked with the National Security Agency to develop a security document which could provide protection of a Windows operating system server, common in many government environments

(Microsoft, 2004). The document contained over 1,000 individual configuration settings, which must be applied to adequately protect the system from misuse or penetration.

In the 1990 study, the National Academy of Science cited the lack of trained personnel and the lack of advanced degree programs in IT security as two causes of poor security within organizations (NAS, 1990). Since then, academic institutions have introduced advanced degree programs and there is an increased emphasis on information security credentials.

Industry has promoted the use of certifications to qualify security professionals as subject matter experts. To date, the credentials are not standardized, do not require similar levels of experience and education, and are not all recognized by other agencies.

Organizations have actively sought to establish credentials of IT security personnel. The Certified Information Systems Security Professional (CISSP) and the Information Systems Security Auditor (ISSA) are just two of the credentials offered to security professionals. In addition, there have been efforts to develop handbooks to provide overviews in the many bodies of knowledge encompassing computer security (Tipton & Krause, 1999). Some federal agencies often require credentials for their security personnel. The current challenge is to standardize the credentials and to establish acceptance and credibility for these credentials.

Another factor contributing to poor IT security is the competition for resources, i.e. security controls, business requirements, or budget constraints. As managers struggle to provide the latest technologies to customers, security professionals struggle to keep intruders from using the internal networks. There will always be a competing goal between providing user information and restricting information, based upon security constraints.

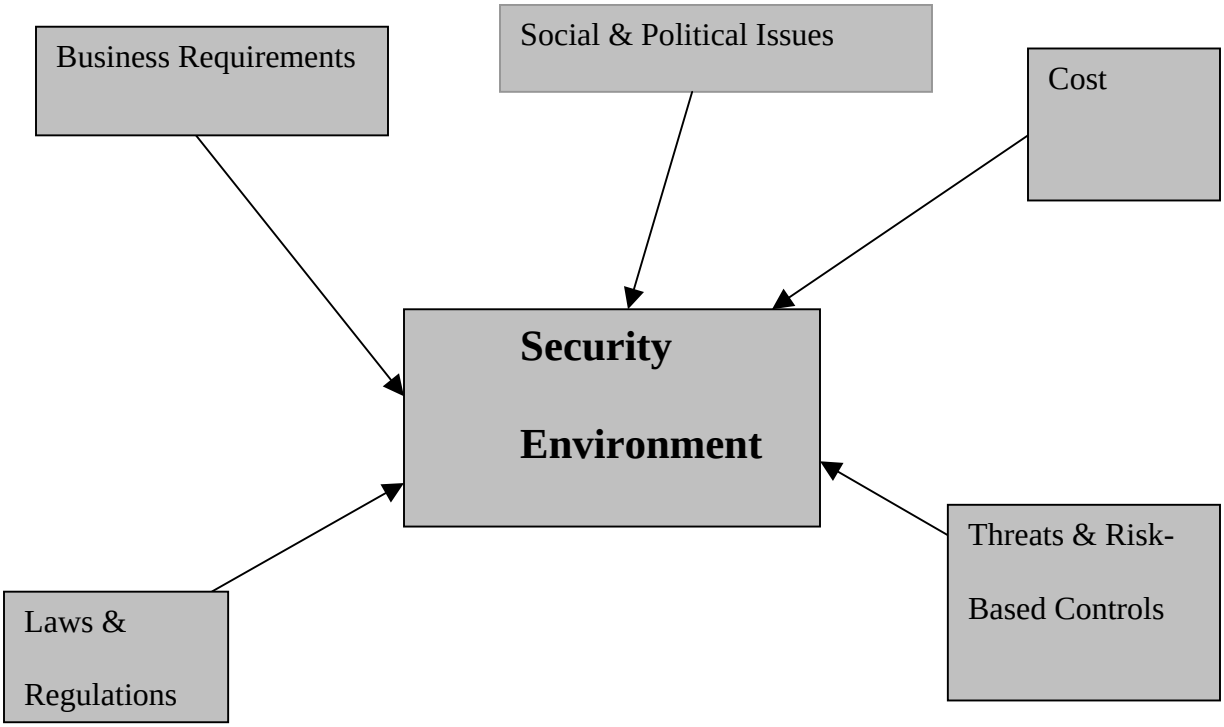
In 2001, federal agencies were chastised for providing functionality, where security controls may have been compromised. Sensitive information was being posted on web sites and

this became so prevalent that agencies were asked to review their information and remove it (Sammon, 2002). The White House had to educate federal agencies to remove sensitive data from web sites, including information on weapons of mass destruction. Security and functionality were competitive resources. In another example, a study was conducted to determine the extent to which sensitive information was posted on the Internet. By keying in the words "Official Use Only" into an Internet search engine tool, there was a 40% confidence interval that sensitive information was actually posted on the Internet, using standard analysis hypothesis tools (Norusis, 2000, p. 235). The two examples illustrate how competing resources can impact how managers implement security controls and potentially impact the security environments.

Newman contends that there are opportunities within the enterprise environment for threats, particularly in the networked environment (Newman, 2003, p.248-249). The primary threats to the organization are: viruses; device failures; internal hackers; equipment theft; external hackers; natural disaster; or industrial espionage (Newman, 2003; FitzGerald, 1999).

Security design and controls will always be dependent upon many factors, including political influence, legal requirements, and business requirements and cost. Figure 1: *Constraints Affecting IT Security Environments* illustrates this concept.

Figure 1: Constraints Affecting Security Environments



With a variety of external factors affecting the security effectiveness, it is crucial to understand exactly how these factors influence the success of IT security programs. This is significant to ensure management understands these and factors these constraints into their own decision-making practices. Using concepts contained in the social process triangle, IT security programs can be influenced by economic, political, and social constraints (Mann, 1995). As this relates to IT security, these constraints all apply but may come in a variety of forms. For example, public laws become a strong political constraint. The significance is that at any given time, one constraint may outweigh the other.

For almost any agency, new programs are being introduced and new computer programs are being written to support the new program efforts. Technology is growing rapidly and IT development must keep pace with the emerging technology, as evidenced by the use of web technologies for federal agencies. As business strives to provide new functionality, this will be a competing resource with IT security initiatives.

Security controls are often implemented depending on the social and political climate. Today, the social climate is very accepting of the need for strong security controls. This can be illustrated with two examples. First, after the terrorist attacks of September 11, 2001, people feared for their own safety. The Department of Homeland Security (DHS) was created and the DHS created a schema for identifying the threat level to US citizens (DHS, 2005). The Patriot Act was then passed, allowing formerly private information to be provided to law enforcement agencies, where related to terrorism. This created a situation in which civil liberty groups stated the government had gone too in invading personal privacy (Lithwick & Turner, 2005). While this may be true, people are more accepting of the situation. Safety is more important than the invasion of privacy to the US public.

The second example has to deal with credit card theft and theft of private information. The use of the Internet has created a tremendous increase in the concept of identity theft, which occurs when someone uses your personal information such as your name, Social Security number, credit card number or other identifying information, without your permission to commit fraud or other crimes, FTC, 2005). The FTC has provided television commercials to warn consumers of this theft and as a result, people are more accepting of using security practices both on the Internet and in daily routines. When security threats go down, it is most likely that people will be less threatened and less concerned about security.

Cost will become a major issue in implanting programs. When programs are not able to be successfully proven using the President's Management Agenda, funding may be cut, adversely impacting the security programs. Budgets are never infinite amounts of money and security will become a competing force with budget initiatives.

Agencies are anxious to develop and implement successful programs. Security can be adversely impacted in two ways. First, program offices will require money for their own initiatives. Second, if money is lost through program offices or money is scarce, functionality controls will be implemented before security controls, to ensure these programs remain in line with the President's Management Agenda.

Some security academics recommend a strong approach to security planning, proposing that resources be properly protected (Newman, 2003, p. 123; Goldman, 1998). There are many issues which make IT security complex:

1) Terrorist attacks are rising and often pose threats to our computer systems and there is a conflict between providing security and ensuring privacy
2) We are faced every day with more sophisticated computer viruses and worms
3) Resources for government agencies will be allocated to successful programs
4) The successful IT security program in government is rare, based upon the current scorecards
5) Federal agencies are failing IT security program efforts
6) IT security often conflicts with business objectives of providing functionality
7) Systems need to be secured, when we have increased threats and less money to fix computers.

Federal agencies must establish a process to enable the current issues to be prioritized, allowing all stakeholders to take part in the prioritization efforts. Public laws will always impact the security environment, as these contain the mandatory requirements for federal agencies. The Federal Information Security Management Act (FISMA), for example, has reporting requirements and specific implementation requirements for federal agencies (NIST, 2005). These laws are currently so complex that NIST has included a FISMA Implementation Project home page to facilitate implementation of the numerous security requirements. Agencies are struggling to implement so many of the current legislative efforts.

Risk assessments will continue to be used, providing risk-based methodologies within federal agencies. As risk assessments are conducted, new threats will be identified. As managers identify threats, IT security managers will continue to focus on the concept of minimizing the threats to systems in a cost effective manner.

Section 3.8 Better Research Methods May Improve Management Controls

There are two feedback loops, which are provided with the IT security process. First, there is a feedback loop from the evaluative process, in the forms of audits. Second, there is a feedback loop generated from identified weaknesses, when systems are exploited or accessed by unauthorized intruders. The evaluative process allows for deficiencies to be corrected before the system is compromised. For federal agencies, managers will benefit from establishing a repeatable process which allows security configurations and policies to be evaluated and changed, as necessary. For example, if a system is penetrated from a computer virus, as soon as the agency receives a “patch” then the security policy will be modified to implement the new corrective controls.

Other organizations are already using automated tools to review system configurations. According to auditors at the American Institute of Certified Public Accountants (AICPA), each year, the government awards billions of dollars in grants, loans, loan guarantees, property, cooperative agreements, interest subsidies, insurance, food commodities, and direct appropriations and federal cost reimbursements which are subject to audit requirements (AICPA, 2005). The AICPA provides guidance relative to government audits, emphasizing that when using the Internet or other methods that the reliability of the information must be ensured. The AICPA provides the governmental policy for audit, Office of Management & Budget (OMB) describing research methods in an audit:

> **"Research and development** (R&D) means all research activities, both basic and applied, and all development activities that are performed by a non-Federal entity. **Research** is defined as a systematic study directed toward fuller scientific knowledge or understanding of the subject studied. The term research also includes activities involving the training of individuals in research techniques where such activities utilize the same facilities as other research and development activities and where such activities are not included in the instruction function. **Development** is the systematic use of knowledge and understanding gained from research directed toward the production of useful materials, devices, systems, or methods, including design and development of prototypes and processes" (OMB, 2003).

As illustrated, agencies are bringing research methods into the field of audit. Better research methods provide better audit reports. Cooper & Schindler define research methods in

terms of validity, reliability, and practicality (Cooper & Schindler, 2003, p.231). If federal agencies are to move to "green" using the President's Management Agenda, managers must understand the advantages and limitations of the various management tools. For example, audits will provide an assessment and a finite point in time. As this relates to continuous monitoring, the audit has limitations. Additional management tools are required.

Commercial organizations have already recognized the need for better management tools, relating to auditing and management controls. First Union, one of the leading banks in the United States, recognized that periodic financial audits provide only a partial picture of the IT security environment (Information Security, 2004).

Management at First Union built a comprehensive plan to involve all organizational IT staffs and business units to build security tools to measure compliance across the organization. This process allows the bank to observe the security posture using an absolute and a relative score. The absolute score shows the compliance against the mandated criteria, while the relative score evaluates the organization against the criteria, taking into account, exceptions to policies.

Other organizations are opting for different management tools and research methods to assess their IT security environments. The National Research Council also published recommendations on maintaining a critical infrastructure, the group also identified the delivery of new digital government services as being dependent on using advanced technology and advised that the government should adopt commercial e-commerce technologies and associated practices, wherever possible (National Research Council, 2002).

The new development in business methodologies shows two areas of concern: 1) how can the value of an audit be improved and 2) how can compliance be continuously measured? This dissertation will focus on improving value within the audit process.

Section 3.9 IT Security Metrics

NIST proposed using metric concepts to enable security programs to be more effectively measured (NIST, 2003). NIST recommends bringing together all stakeholders, including stakeholders from other business functions. By establishing metrics, management personnel can measure the effectiveness of performance of security controls.

This tool is good for measuring ongoing compliance but does not provide a scheme to allow existing issues to be prioritized. The current NIST metric process remains a high-level assessment tool and does not include metrics for detailed findings, which would be contained in an audit report (NIST, 2002). For example, using the NIST metric forum, an agency will be able to identify the number of systems certified and accredited but will not identify detailed information, such as the use of passwords, within the system. This metrics will provide a generic perspective of the enterprise environment.

Robert Frances Group (RFG) believes security metrics are essential in the IT security organization. In a recent survey on security metrics practices in the enterprise, RFG found that nearly all participants collected and reported these metrics, but only a subset of the participants felt these practices were effective (Robinson, 2005). While this may provide a management perspective, this metrics is currently not sufficient to measure or evaluate the IT security environment, as an audit can accomplish.

Section 3.10 Risk Assessment Methods

Risk assessments allow organizations to prioritize security controls, based upon cost and risk (Tipton & Krause, 2000, p. 247-249). Tipton and Krause recommend evaluating questions relative to the organization, such as: 1) what could happen; 2) if it happened, how bad could it

be; 3) how often could it happen; and 4) how certain are the answers to the first three questions. Annual loss expectancies are then calculated and used to evaluate the cost of a computing resource with the cost of the expected loss and the cost of the projected solution.

Section 3.11 Summary of Literature Review

Federal agencies are currently faced with challenges relative to IT security problems. The agencies must continue to provide increased technology to its customers yet Congress faults agencies with providing increased technology, without also providing greater security.

Chapter 4: Conceptual Framework

The framework for this study is that there must be quality within the audit process. For this study, quality is explored using concepts of validity, reliability, and practicality (Cooper & Schindler, p.231). IT security is not easily evaluated yet there is a critical need, when agencies are faced with funding constraints based upon a program's success or failure. The President's Management Agenda states that resources should be allocated to programs which deliver results (OMB, 2002).

Results are difficult to quantify for IT security initiatives. IT security provides for confidentiality, integrity, and availability yet by itself, IT security is not viewed as a product or service. How can the success of the program be measured, if it does not stand alone? Performance provides a measure for IT security programs. As a key indicator of program success, it is important that the evaluation processes and techniques be effective not only in evaluating program success but also in allowing problems to be prioritized for easier correction.

In using the President's Management Agenda, there must be a mechanism in place to allow federal agencies to show success relative to IT security. Cost will not be a good performance indicator.

Some of the cost-implications related to implementing IT security follow: 1) Security represents a cost of doing business; 2) Security is akin to insurance costs; 3) New e-business revenue streams may depend on proper security; 4) Security is one aspect of risk management; 5) Legal actions might result from failure to meet a general duty of care manifest as minimum security standards; 6) Current resistance to security expenditure will shrink as the information age matures; after all, nobody questions the cost of building security anymore (Commerce,

2003). All of these factors will adversely impact management choosing cost as a performance indicator, since there are many unknown and unquantifiable issues.

Agencies can use metric-related concepts as performance indicators. For example, if federal agencies implement IT security controls, a performance indicator would be obtained by evaluating the level of compliance. 90% compliance would earn a score of A. 80% compliance would earn the score of B and so forth. Similarly, if an agency conducted an evaluation and/or audit of an IT security environment, the audit should be able to show a level of compliance, using percentages. This will be used to determine if audit reports provide a performance measure. These performance measures will directly relate to evaluating audit reports, allowing statistical samples to show representations of compliance using percentage indicators.

Feedback provides the organizational learning. By using feedback mechanisms, a federal agency can identify key problem areas, focus on the key problem areas, and correct these in the future, as necessary based upon cost and risk. The primary concept is that audit reports must provide sufficient information to allow the agency to learn about the significant issues and concerns. If the audit reports contain only a bulleted list of observations, this is not information but merely data, which has not been analyzed.

Chapter 5: Research Methodology

The purpose of this study was to evaluate audit reports over a two-year period to determine if the reports provided an effective assessment of a federal agency and to determine if the reports used research methods, such as validity, reliability, and practicality. The process evaluated with this study was taken from the FISCAM manual, defined by GAO as the primary tool, used by the auditor. In addition, the feedback process was evaluated. This study examined audit reports and assessed if management learned from feedback mechanisms, in the form of date contained within audit reports.

In conducting an IT security audit, general controls were viewed as the structure, policies, and procedures, applying to the computer operations (GAO, 1999, p. 3-1). The GAO reviewed six categories of general controls, as part of the audit, including: 1) security planning and management; 2) access controls; 3) application development and change controls; 4) system software; 5) segregation of duties; and 6) service continuity.

For each of these component areas, the *Federal Information Security Controls Audit Manual* (FISCAM) procedures provided a standard list, which are GAO recommendations, for testing and to validating general controls (GAO, 1999). Examples of these procedures included:

- Review pertinent policies and procedures;
- Interview management and systems personnel;
- Observe personnel; identify opportunities to adversely impact the operating system, and
- Search password files, using audit software (GAO, 1999, pp. 3-77, 3-78, 3-79).

Note: This study uses the 1999 FISCAM manual. Though the manual has been republished, GAO has identified that no content has been changed; the only changes were formatting issues (GAO, 2004). FISCAM provides the audit standards and requirements for the GAO to conduct audits of federal agencies.

GAO reports formatted findings by providing background information, descriptions of criteria, and information relative to the finding. For consistency, the GAO used consistent language to identify the scope. For example, the GAO described the purpose of evaluating information system controls in the following manner: 1) protect data and software from unauthorized access; 2) prevent the introduction of unauthorized changes to application and system software; 3) provide segregation of duties involving application programming, system programming, computer operations, information security, and quality assurance; 4) ensure recovery of computer processing operations in case of disaster or other unexpected interruption; and 5) ensure an adequate information security management program (GAO, 2004, p. 6).

This study evaluated audit reports conducted by GAO, focusing on reports published between September 11, 2001 and December 31, 2003. September 11, 2001 was chosen as the starting period, since the threat of terrorism and cyber terrorism became a major concern for federal agencies. For this study, one report was included from January 2004, since this reported information obtained from 2003. The concluding date for the study was December 2003, since 2004 data was not yet available.

There were two hundred and six (206) individual findings evaluated, from six different GAO reports, within this dissertation. This data is contained in the Appendix 2 *GAO Reports and Associated Findings.* The primary goal of this study was to determine the extent to which GAO reports used basic research methods, as described in *Business Research Methods (*Cooper &

Schindler, 2003, p.19). The assumption was that by using better research methods, managers would be able to have better information available and make better decisions. The *Federal Information Systems Control Manual, GAO/AIMD-12.19.6* identified the control techniques used by GAO to conduct audits for federal agencies and was used to obtain clarification on the GAO audit process.

Audit reports were retrieved from the GAO web site, located at www.gao.gov. All public versions of the GAO reports were available from this site. An Internet search was made on the GAO web site to obtain a list of all reports with the criteria IT Security. For example, in the search of audit reports, *GAO-04-483T Information Security: Continued Efforts Needed to Sustain Progress in Implementing Statutory Requirements* was retrieved. These reports were then downloaded to the personal computer and/or requested via hard copy from GAO personnel using the GAO web site.

Documents used for this study fell within the specified time-period. The GAO reports were broken down into the following sections: Results in Brief; Background; Objectives, Scope, and Methodology; Findings; Conclusions; and Recommendations. The Background section was reviewed to understand the scope and intent of the audit. The Findings section of the audit report contained actual findings and information. This section contained the primary data used for this study. In addition, the following information was collected:

- Report title
- Organizational size, including the number of employees, number of offices, number of states, relative to the organization
- Number of users on the system evaluated
- The GAO criteria used to evaluate the agency

- The associated findings for the criteria. For example, one criteria could result in multiple findings
- The number of occurrences, the finding was observed by the GAO
- The percent of the occurrences, as this related to the total environment.

Practicality was evaluated by determining how well a single GAO report could be understood by multiple readers. In reviewing the report, the question was asked, "Could anyone with sound logical skills understand what the report intended to portray?" One report was selected at random from the GAO reports. In this example, the word "system" was selectively captured. Often, the word system was used in multiple contexts. For each time the word system was used, the following information was captured:

- Page the word was located on within the study
- The sentence containing the word "system"
- The number of times the single word was used within a single sentence
- The context of the meaning for the word "system"
- A general category, providing the definition.

At this point, an arbitrary category was set up for this study to better classify the context of the word. For this study, the categories included: enterprise system; network/operating system; networked controls; operating system; application system; roles of an employee; and business system. These categories were selected, based upon the multiple uses of the word, related to one of these categories. The purpose of this small study was to determine if a GAO report would have the same meaning, when read by multiple people.

Section 5.1 Evaluate Audit Process

The purpose of this study was to evaluate the GAO audit reports and to determine if these provided a valid, standard, and reasonable assessment of an agency's IT security environment. Specifically, findings were evaluated to determine how adequately these findings describe or define the situation at hand, i.e. the problem being defined. This study used concepts of business research methods, including validity, reliability, and practicality (Cooper & Schindler, p.231-235).

As federal agencies become more accountable, per the President's Management Agenda (OMC, 2003), federal agencies need to integrate better management practices into the performance measures of these programs. This study focused on how the audit process could be improved and to move into line with the President's Management Agenda.

Cooper & Schindler stated that the ideal study should be designed and controlled to allow for precise and unambiguous measurement of variables (Cooper & Schindler, p.229). The characteristics of a good measurement were defined in terms of validity, reliability, and practicality.

Validity is the extent to which a test measured what we attempted to measure, i.e. making sure the evidence is relevant to the question being asked (Cooper & Schindler, p. 231). As an example, if auditors were studying the number of different controls on a computer network of federal agencies, there would be no relevance to collect information regarding the controls of a computer network in a school system. The school system outside the scope of federal agencies and would not be relevant.

Within the concept of validity, Cooper and Schindler discussed three sub-components: content validity; criterion validity; and construct validity. *Content validity* related to how

adequately the questions or assessments measure the environment being studied and ensure all questions are relevant to the subject-area. *Criterion validity* related to how well a question can predict an estimate or a condition. Not only must the criteria be clear but also the information must be available, to predict a condition or state of being. For example, if weak general controls are measured, can these measurements be used to predict and generalize the statement that weak controls exist across the entire environment? *Construct validity* ensured that abstract concepts, which are studied, will have similar meaning to all researchers. If an audit measured general controls of a "system", would the concept of a system be understood, in the same way, for each reader of the audit report (Cooper & Schindler, p.234)?

Reliability allowed for the standard measurement of an observation. While a research study may provide valid questions, unless the measurement tool is consistent, the results will not be reliable (Cooper, p. 236). For example, two different audits should enable comparable and similar results to be obtained, due to the consistency and repeatability of the audit procedures and measurement tools. Additionally, if two different auditors were to conduct an audit of the same organization, the findings should be very similar due to the reliability and standard application of the measurement tool.

Practicality ensures that there are reasonableness constraints for the audit, relative to time, money, and resources used to conduct an audit (Cooper & Schindler, p. 240). An audit should not take place for an infinite amount of time and with unlimited resources, since this is not reasonable. Additionally, practicality relates to the usefulness of the study. Does the audit report present itself in a format, which can be understood by all readers? When an audit report is issued, the reader should be able to read the report and observe similar conclusions, even when ready by two or more different groups (Cooper, p. 240).

By integrating these concepts into an audit report, performance metrics are provided. The level of compliance can be assessed using performance metrics. In addition, by using these concepts, the context of the information can be readily understood, allowing federal agencies to learn via the feedback process and focus on key areas of concern, based upon the findings contained in the audit reports, i.e. which findings were most significant.

The study assumes the following: 1) GAO should provide a high-quality, independent assessment of IT security programs 2) reports provide federal agencies with sufficient information to correct IT security problems and 3) GAO reports provide a feedback mechanism to allow another agency to learn from the mistakes of another agency.

Chapter 6 Discussion and Results

The following chapter will provide a discussion of the study, identifying some of key findings of the GAO reports, and summarizing the results and conclusions.

Section 6.1 GAO Reports Lack Validity

Statistical sampling provides the assurance that the instances identified in the audit represent the actual environment being evaluated. When statistical sampling is not used, the validity of reports may be questioned.

For most IT security audits, the GAO does not use statistical sampling. Network components are chosen. If a problem is identified in several locations, the GAO assumes that this is a persistent problem and that it occurs throughout the organization. In addition, the GAO has cited that network capabilities enable network configurations to be captured and analyzed without using sampling methodologies. The GAO currently relies on evaluating network configurations, which reside on the network. This is accomplished by examining the system configuration of a particular system and identifying the specific configuration policies. If a number of instances indicate a policy is incorrect, the GAO may assume that the problem is persistent through the organization.

There are two problems identified in the GAO audits due to the lack of sampling. First, there is no knowledge regarding the number of occurrences. Second, the number of occurrences cannot be placed into perspective, since the total population being evaluated was not defined.

To illustrate this concept, assume that a computer is found “unattended.” The unattended computer is an instance of failed criteria (all computers should be attended represents the criteria). While this instance is certainly true, it cannot be assumed that all computers in the organization are unattended.

In GAO reports, sampling is not used for IT security audits (GAO, 2004, November 29). For example, the GAO conducted an audit, GAO-01-751 *Information Security: Weaknesses Place Commerce Data and Operations at Serious Risk (GAO, 2001).* Within the report, the GAO identified the target population as the Department of Commerce, which contained seven agencies. Within the GAO report, the GAO described a typical agency as one agency located in 50 states and located within 80 countries. Within this agency, the agency had IT systems. The typical agency had 155 local area networks and over 3,000 users (GAO, 2001). For this particular audit, the GAO identified the objective as providing an evaluation of the entire Department of Commerce, including all seven agencies.

Using this report, the GAO report does not adequately define the universe or target population being evaluated. For example, the GAO indicated the auditors reviewed 120 systems, including firewalls, routers, switches, and servers. The sample was then identified as: 8 firewalls, 20 routers, 15 switches, and 3 agency's servers.

This causes confusion for three reasons. First, the report alluded to the network as the system concept. There was never a statement identifying hardware or network components as systems. Second, if these components were used to assess the configurations, the sample size is too small to be statistically valid. Third, there is no population size defined to establish the relevance. For example, if 8 firewalls were not in compliance, what was the total number of firewalls contained within an agency?

In another example, the GAO defined the target population as seven agencies, with the typical agency maintaining locations in over 130 dispersed geographical areas. For this GAO audit, the GAO visited one geographical area, which was located in the District of Columbia

metropolitan area. A situation identified in D.C. cannot immediately be summarized as a systemic problem with the entire organization, where the organization is located in 130 locations.

In yet another example, the GAO identified problems with user accounts. While the user accounts presented a problem, the GAO did not define the total number of users being evaluated or the percentage of times the user problems occurred.

In general, for most GAO reports, there was not a sample size identified for review nor was there a population size identified as the total population being evaluated. For this reason, using the validity constructs identified by Cooper & Schindler, the GAO reports do not meet concepts of validity, where the target population has not been properly established.

Section 6.2 GAO Reports Lack Reliability

The reliability of GAO reports is a second concern. After reviewing over 200 findings in six GAO reports, the reliability of findings became a concern. The reliability is demonstrated using the same example as used above: Report: GAO-01-751 *Information Security: Weaknesses Place Commerce Data and Operations at Serious Risk (GAO, 2001).* While this report illustrates one example, the data contained in Appendix 2 illustrates this practice for many of the GAO findings.

Below, Table 2: *Department of Commerce Population Size versus Sample Size* illustrates the sample sizes and population sizes used to evaluate IT security concepts. For example, the number of locations identified in the audit was 130; the sample size was 1. In this example, the sample sizes do not always provide a large enough number to provide a statistical representation of the entire population. In this report, several sample sizes were identified as 7, 1, and 1. In using the Cooper & Schindler methodologies, the sample sizes are not sufficient to allow a generalized statement to be made about any observations. In this report, the GAO stated that

Commerce was not adequately protecting access to the network, specifically in managing user IDS, passwords, dial-in access, or configuring network servers. For this finding, the GAO did not establish the number of samples taken to make this generalization. In addition, the population base being evaluated was also not established. In this particular example, using Cooper & Schindler's methodologies, the finding is neither valid nor reliable.

Table 2: Department of Commerce Population Size versus Sample Size (GAO, 2001).

Defined Population	**Population Size**	**Sample Size**
Bureaus	7	7
Size of 1 Bureau		
# Locations	130	1
# Countries	80	1
# Local area networks	155	
# Users	3,000	
Systems[1]	94	120
Firewalls	Not defined	8
Routers	Not defined	20
Switches	Not defined	15
Servers	Not defined	3

[1] The sample size being greater than the population size is an extract from the GAO report.

Within Table 2, the evaluation of systems shows another example, when GAO identified the sample size as larger than the population size. The sample size is 120 systems yet the report stated the Department of Commerce hosted only 94 systems.

Figure 2: Ratio of Findings, Population Size/Universe, and Unknown Number of Occurrences

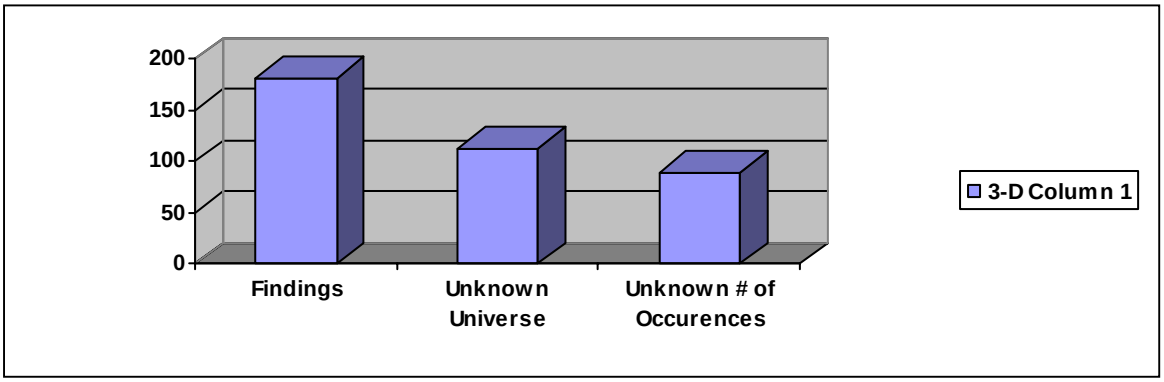


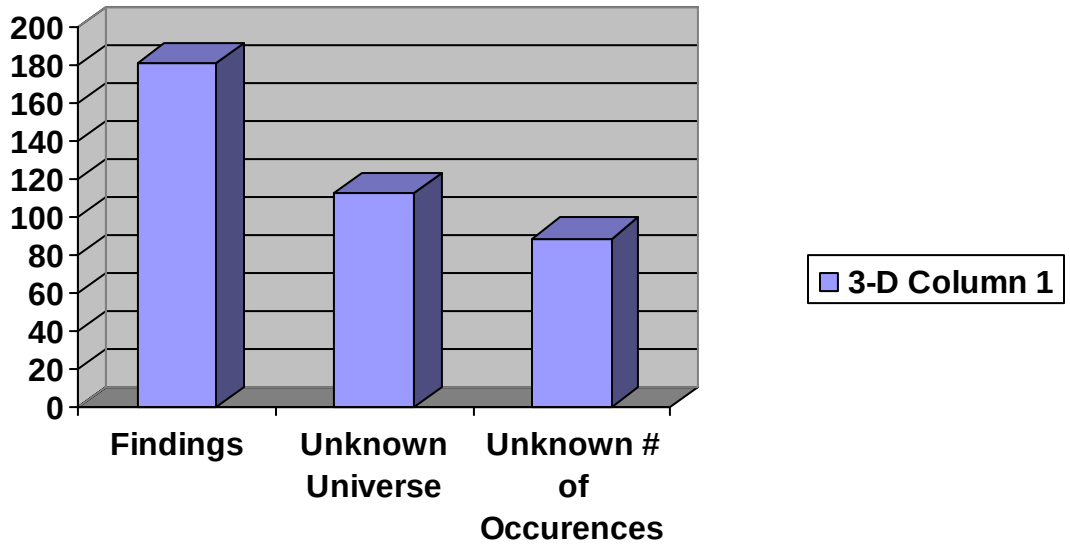
Figure 2, *Ratio of Findings, Population Size/Universe, and Unknown Number of Occurrences,* illustrates potential problems in understanding the context of GAO findings. The study found that GAO sometimes identified conditions, without providing relevant information. For example, sometimes a finding would be identified but would not identify the number of times this occurred. In other instances a finding was defined with a number of occurrences but there was no population/universe defined so the context could not be understood.

Of the 206 findings reviewed, the actual target population being evaluated was not defined for 113 of the findings. Conversely, in 89 instances, the GAO defined findings without identifying the number of times a situation occurred. For example, the GAO identified findings using phrases such as 'some of the time, some users did not use passwords.' The importance of this statement is that the context of the finding cannot be understood, without understanding the

target population, the number of observations, or the percentage of observations relative to the population.

Figure 3: *Universal/Population Sizes for Specific Reports* demonstrates the number of findings and the relationships between undefined universes or sample sizes. In this example, for 181 findings written by GAO, in 113 instances, the universe being evaluated was not defined. In 89 of the instances, the number of occurrences was not defined.

Figure 3: Universe/Population Sizes with Specific Reports



In this example, the GAO made statements and established findings without all of the required information. For example, in one GAO report, the GAO determined systems administrator privileges were granted to an excessive number of users. In this instance, the GAO identified 20 users with these privileges. The problem with the finding is that there is no knowledge of the total number of users who were on the system. If the total number of users was 100, 20% of system administration users might be considered high. If the total number of users

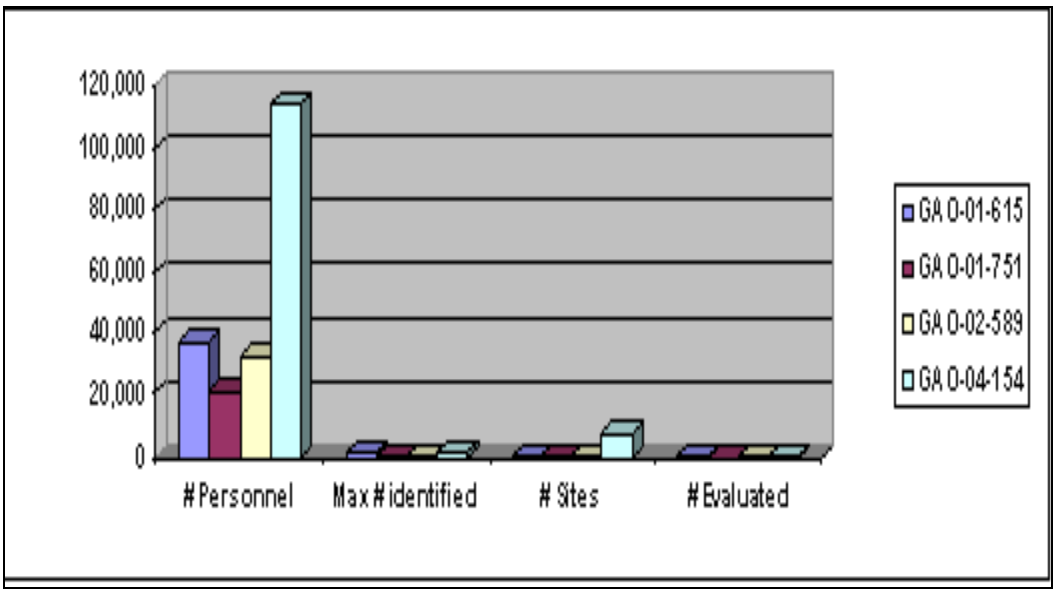
was 1,000, this represents only 2% of the population. Since the total number of users is never provided, an agency cannot assess the true significance of this finding.

In the second portion of the chart, there is no number of occurrences established. In this GAO report, the GAO identified people having access to the building, without using an access card, by following anther person into the building. The GAO report wrote the finding as 'people were able to access the building.' It is difficult to understand the extent of the problem since the number of occurrences is not known.

Figure 4: *Sample Sizes with Specific Reports* shows that when the universe has been established within a GAO report, a sample is not used to establish IT security findings. In this example, the GAO identified findings related to the number of personnel. For these findings, there was rarely a population size identified for the personnel being evaluated, Max # identified. The number of personnel evaluated always took place at almost a single location, where there were 130 locations. In addition, the number of findings, which identified a number of occurrences, was almost non-existent.

Appendix 3: *GAO Reports and Associated Findings* contain the data used to support these graphs and include the statements made within this study.

Figure 4: Sample Sizes with Specific Reports



Section 6.3 GAO Reports Lack Practicality

In addition to factors of validity and reliability, Cooper & Schindler discuss the concept of practicality, which ensures that a report will be understood similarly when read by different people. To determine the practicality and readability, one GAO report was used to determine if the concepts were clearly defined and would be easily understood by different people. Though terms were not clearly understood in other reports, this GAO report emphasizes the problem of using the same terms that contain multiple meanings.

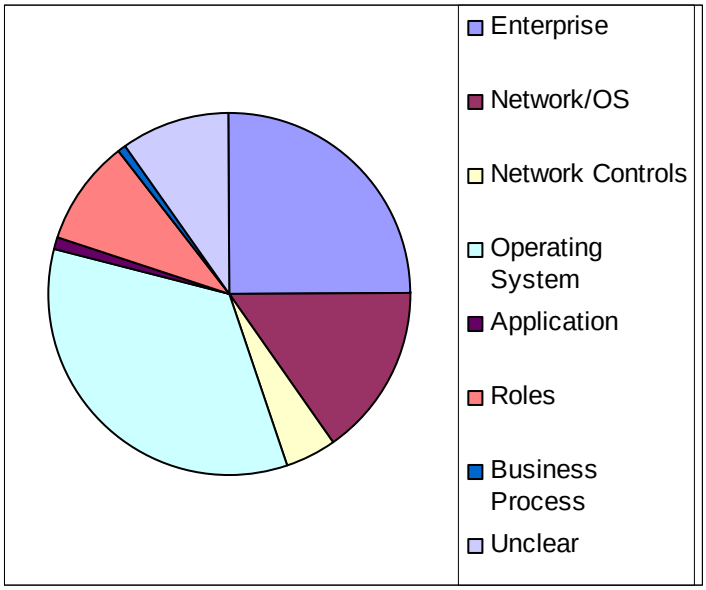
The report used GAO-01-1004T *Information Security: Weaknesses Place Commerce Data and Operations at Serious Risk.* This report is often confusing and difficult to read, due to the lack of standard definitions and terminology. In this example, the word "system" was used to mean many different concepts. In the 36 page report, the GAO uses the word system 307 times, but not always meaning the same thing. By not establishing standard terms, it was never clear in what context the word "system" was being used. In one instance, "system" was used six times in a single sentence, but not always referring to the same concept. The significance is that the report

cannot be easily used if it is difficult to read. More importantly, if managers read the same report yet come to different understanding, there is no common language for IT security professions, which enable better communication of existing problems.

To illustrate this, the word "system" was arbitrarily grouped into categories, including: 1) Enterprise System, which relates to an entire information system of an agency; 2) Network/OS, which includes controls that relate interchangeable between the network and operating system; 3) Network Controls, including network specific issues; 4) Operating System, including operating system specific issues; 5) Application, including application program and application program controls; 6) Roles, including specific responsibilities related to the environment, such as system administration; 7) Business Processes, including operations and daily controls; and 8) Unclear, including system concepts that were not easily discernable. The intent was to demonstrate how there could be potential confusion by using the same word, when the word took on different meanings within the report.

Figure 5: *System Definitions*, shows the number of times the word system was used in one report to relate to one of these areas. As illustrated in Figure 4, there are multiple interpretations, by using one word to describe different concepts. As a result, this can cause confusion and misunderstanding when interpreted by different people. Within Figure 4, the number of times the word "system" was used for each of these categories was: Enterprise = 77; Network/OS = 47; Network Controls = 13; Operating System = 105; Application = 4; Roles = 2; Business = 2; and Unclear meaning =30. The total number of times the word "system" was used was 307 times in the 36 page report.

Figure 5: Use of System Definitions and # of Times Used



Auditors must establish and use standard and consistent language within audit and evaluation reports; otherwise there is no way to achieve a common understanding of the problems. Appendix 2: *Key: Definitions of the Word "System" Within 1 GAO Report* contains the data used in the study, where multiple uses of the word system were used. The ambiguous language of GAO reports caused additional concerns for readability of reports.

In addition to the interchangeable use of different words or terms, GAO reports are not always logically presented to allow the situation to be understood. In one example, the following text is used to describe a situation at a federal agency:

> "All Commerce bureaus reviewed were not effectively managing user IDs and passwords to sufficiently reduce the risk that intruders could gain unauthorized access to its information systems to (1) change system access and other rules, (2) potentially read, modify, or delete or

> redirect network traffic, and (3) read, modify, and delete sensitive information. Specifically, systems were either configured to require passwords, or if passwords were required, they were relatively easy to guess.
>
> 1) Within the access controls portion of the review, access controls were defined as inadequate. Two examples follow: 1) Administrator accounts did not require passwords and 2) Systems allowed users to change passwords to a blank password (GAO, 2001)."

Using this example, the reader cannot understand the intent of the meaning, as this presents a logical ambiguity. The following questions may be raised: 1) How many of the accounts did not require passwords or allowed a blank password? 2) Since there are 3,000 users, there is a need to understand the context of the problem. 3) Is this a small percentage, i.e. under 1% or a persistent problem throughout the network? With the current statement, there is no way to determine the actual security condition, relative to the population or relative to the other findings.

This situation was addressed to the GAO. They responded that since this was a critical finding, the 1% situation would always be significant. There is 100% compliance for these scenarios. The ambiguity issue was not addressed. This situation creates a situation in which there is never a baseline measure from beginning to an end result. This methodology does not allow a manager to distinguish between a policy aberration or a systemic problem. Without this information, there is little value to the finding.

Section 6.4 Lack Prioritization

As the federal agencies struggle to implement security, agencies are continually faced with resource constraints. When there is a 100% compliance rule, agencies will be challenged with prioritizing which problems are most critical to correct. In addition, business organizations will compete for resources, either to provide more functionality or to fix security. There must be a strategic plan and process to allow the most significant needs to be addressed first. In addition, the plan must allow mangers to prioritize and to allow for vetting by all stakeholders within an agency. The GAO takes the position that the agency has the responsibility to prioritize findings and identify corrective procedures.

Section 6.5 GAO Process Does Not Allow for Feedback Mechanisms

Audit reports should be able to use feedback to improve future controls. As this relates to IT security, this feedback process allows other groups and agencies to learn from their own mistakes or mistakes of others and to make improvements in their own IT security programs, based upon these mistakes.

Feedback can be provided to an agency by allowing a federal agency to understand the significant issues of an audit report. For example, if an agency is attempting to improve IT security, one could review another audit report and search for the critical failure points, experienced by other agencies. The management teams could then focus on critical areas and fix those areas first, within their own organization. If a federal agency is audited but every finding is determined to be critical, if there are many findings or issues, a learning organization cannot easily understand which findings are most critical to correct. This can be illustrated using the report GAO-03-564T *Information Security: Progress Made but Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures.* In this report, twenty-two points were

identified related to access controls. GAO identified some of the following: network not configured in accordance with security policies, default vendor accounts being used, password settings incorrect, agencies do not always update software, and Intrusion Detection Systems (IDS) not implemented at all sites. If an agency wanted to improve security within the internal organization using this report, there is no easy way to determine what issues made a network more vulnerable. There is no easy way to determine which situations occurred most frequently, since the number of occurrences was not defined. There is no way to understand how this impacted the organization because there is no discussion of the population sizes or the percentage of the times different situations occurred. Using only five items within the report, this demonstrates a problem with being able to use information to enable organizational learning to occur.

The need to allow organizational learning from GAO reports was identified to the GAO. The GAO reported that GAO reports were never intended to provide value to other organizations. The reports were only intended to provide an evaluation to the individual agency. The GAO also reported that individual agencies have all of the necessary information, detailed within the Limited Official Use only version of the report.

Without valid assessment processes, the feedback and learning process is challenged, even for the agency holding the audit report.

Section 6.6 Results

The results of this study of IT security in the federal government follow. First, federal agencies are unable to effectively implement and manage their IT security programs. As discussed in Section 3.1, federal agencies have continuously been faced with implementation requirements of complex and voluminous IT security requirements but have been unsuccessful in

accomplishing this. Second, the answers to the questions related to the quality of GAO reports showed that: 1) GAO reports did not provide a high-quality, independent assessment of IT security programs, 2) reports do not provide federal agencies with sufficient information to correct IT security problems and 3) GAO reports do not provide a feedback mechanism to allow another agency to learn from the mistakes of another agency. Third, GAO reports do not allow for findings to be prioritized by criticality. Techniques such as the Ten Step Security Delphi Model, discussed in Appendix 5 can be used to enable findings to be prioritized and better managed. Other organizations are already working to improve the quality of the audit process (AICIPA. 2004).

Chapter 7 Recommendations for Improvement

Recognizing the GAO process may not change, individual agencies must take responsibility for ensuring the security of their own IT environments. While evaluations and audits provide excellent venues for assessing IT security programs, the quality of IT security audits must be improved, if these are to add value to the organization. By integrating concepts from this dissertation, federal agencies may be able to improve the quality of individual agency audits and evaluations. These recommendations fit within the scope of the FISCAM audit manual and are also compliant with the guidance provided by the AICPA.

As technology increases, management requires better analysis and decision-making tools, relative to implementation of IT security concepts. Analysis and decision-making tools provide capabilities of providing more valid assessments of an agency. State agencies are already integrating measurement tools into the audit process. For example, the Florida Department of Revenue is using concepts of electronic auditing or e-Auditing, a computer-assisted auditing tool that uses electronic records to complete all or part of the audit. For Floridians, if you use a computer system to record business activity and maintain data electronically, you are a candidate for an electronic audit (Florida, 2005). In addition, the Department of Revenue has purchased software tools to perform electronic data conversion and analysis, allowing statistical sampling to be used (Florida, 2005). This allows valid samples to be used as part of the general audit.

Federal agencies must work toward practices that are being used by state agencies. These practices will provide the consistency necessary for conducting IT security audits. In addition, if federal agencies are audited, automated tools provide more reliable data to support an agency's position.

In addition, state agencies have already recognized the need to use automated tools and techniques to provide additional evaluations of IT security (AICIPA. 2004). Federal agencies must take responsibility for its own IT environments and provide individual evaluations and assessments, using best practices from other organizations. Specific recommendations are provided below.

Section 7.1 Require Statistically-Based Findings

Some GAO audit reports provided statistically-based findings. Two reports using better sampling are contained in *GAO-02-676T Government Purchase Cards: Control Weaknesses Expose Agencies to Fraud and Abuse* (GAO, 2002).

In the report section from the audit: *GAO-02-676T Government Purchase Cards: Control Weaknesses Expose Agencies to Fraud and Abuse* (GAO, 2002), the review process of purchase cards is in question. The GAO review criteria states "transactions and other significant events should be authorized and executed only by persons acting within the scope of their authority" (GAO, 2002). The GAO finding states that the use of the oversight tool in the Purchase Card Management System has not been effectively implemented. The supporting evidence states that according to Agriculture's Inspector General, only about 29,600 out of 50,500 alerts in the database had been read. This calculates to 59.5%.

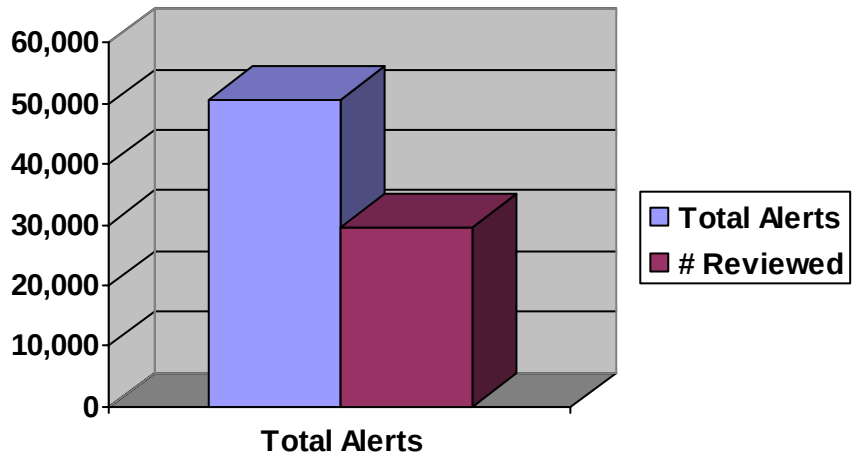
GAO personnel stated that type of sampling was not relevant in an IT security audit and the need to prioritize findings was not a role of the auditor (GAO meeting, 2004). However, within this example, there is a clear criteria stating actions must be reviewed. In addition, the GAO report has identified a total population size of 50,500 alerts in a database. From this, the entire database was reviewed and the GAO reports notes that only 29,600 were reviewed. The entire population is readily understood and we can determine not only that this is a significant

number but immediately determine the percentage this represents of the total population, i.e. 59%.

In this example, even if the entire population was not easily discerned from the report, the report also provides an actual count, i.e. 29,600. This represents not only a valid sample size but also a definitive number. This report results in a clear understanding of the expectation and the current condition.

Figure 5 *Diagram of Purchase Card Alert System Showing Number of Alerts versus Number of Alerts Reviewed* illustrates how using a statistically-based finding makes information easier to understand. In this figure, there are 50,000 alerts identified and 29,600 reviewed. The significance of this is that management can better assess the finding and to determine the extent of the problem and potentially make a better decision on whether or not to correct the problem.

Figure 5: Diagram of Purchase Card Alert System Showing Number of Alerts versus Number of Alerts Reviewed



Without this critical information, it is impossible for an agency to look at multiple findings and identify which findings present the most risk and to identify which findings should be corrected first, based upon a risk.

Section 7.2 Require Stronger Research Methods to Assess Federal Agencies

For any federal agency, audits and independent reviews are crucial to the agency. It is only through the independent testing, assessments, and auditing, that problems can be discovered and corrected. It is important for the federal agencies to be able to understand exactly what the audit reports are stating. This information must contain specific information, to allow the agency to understand: 1) the criteria use to evaluate an agency; 2) the population being evaluated; 3) the sample size used to review the target population; 4) the extent the findings impact the agency, i.e. the actual number of occurrences, relative to the total population.

For example, if a finding states 1) there were some instances of alerts not being reviewed; or 2) there were many instances of alerts not being reviewed, the finding is not clear. It does not clarify 1) the extent of the problem or the situation at hand or 2) if the problem is an aberration or a systemic problem. Within all federal agencies, better research methods are required to maximize the value of IT security audits. Specifically, auditors must address concerns of validity, reliability, and practicality.

To improve validity, auditors must identify the target population being evaluated and the sampling criteria. Auditors must be able to look at the target population and/or universe and apply statistical sampling methods to obtain a solid sample size for the environment being evaluated. It is not sufficient to identify that there are several occurrences of an instance, unless this can be correlated back to the entire population and to show that the sampling provided a sample, which provides less room for error.

Reliability can be improved by implementing procedures which provide not only the information required to support a finding but include information to support the pass and failure rate of a finding, the process used to ensure repeatability, and other standardization methods.

Auditors must identify baseline criteria. For each set of criteria expected results must be identified. Two different audits for the same criteria should not yield dissimilar results. There is no room for discussion on correcting these, even within the same agency, since the results are not stable relative to the criteria. In addition, definitions need to be more consistently defined and used within the audit reports. Unless audit reports provide more value to federal agencies, these reports lose credibility and become a paper management tool rather than an assessment tool.

Section 7.3 Require Feedback Mechanisms

One of the mechanisms used by organizations to become learning organizations is to learn from mistakes, through feedback loops (Senge 2005). Within IT security, feedback loops can be obtained from two sources, either from an audit or from an unauthorized intruder. By using audits, agencies can learn from the audit process and learn in a situation, which does not compromise the system.

One mechanism for agencies to improve feedback processes is to ensure audit reports are written to ensure there is a thorough understanding of the situation. In this way, other agencies and other organizations could learn from currently published audit reports. Two suggestions are identified below:

a) Clarify definitions so that terms are better understood. If there is confusion, agencies can use hyphenated words, a glossary, or other mechanisms to clarify vocabulary

b) Within the reports, provide relativity to the findings. While an audit report may not want to specify exact numbers or percentages, due to the sensitivity, an agency can

report for example, a high-risk finding was identified, which demonstrated that passwords were blank. This was a low-occurrence rate for the agency.

Internal assessments should, of course contain accurate measures, sample sizes, etc. By using an improved audit process, a federal agency will have the opportunity to better improve the posture of an IT security, by allowing resources to be dedicated to systemic problems.

Section 7.4 Require Prioritization of Weaknesses

Prioritization allows critical/high-risk weaknesses to be identified first, followed by moderate risk weaknesses, and finally by low-risk weaknesses. With a prioritization process, audit reports could and should provide a basis or scoring to allow an agency to determine the relativity of the weaknesses, to the entire infrastructure and relative to the other weaknesses.

A sample table has been generated to illustrate how findings could be ranked and prioritized within an audit report, by an audit agency. In using the table, the first finding identifies an unlocked computer room. Using a prioritization process, a manager can observe that this has been identified as a high-risk to the organization. In addition, the manager can observe that this is more than a single occurrence and that this has occurred in 50% of the population.

By using this table, with a prioritization, management could determine that this is not only a finding but a systemic problem and management would hopefully determine that the resources should be assigned to fix a high-risk finding, which is also the most prevalent problem in the organization. Table3: *Sample Ranking of Security-Related Weaknesses* illustrates how weaknesses and/or findings may be prioritized. Risk levels can be determined using a consensus-based approach.

Table 3: Sample Ranking of Security-Related Weaknesses

Risk Level	Finding	Percentage	Total Population
High	Door to computer room was unlocked	50%	2 doors
High	Root privileges were given to many users on Windows systems	20% or 100 users	500 users
High	Root privileges were given to many users on Unix systems	1% or 5 users	500 users
High	Blank passwords were discovered on the system	1% or 5 users	500 users
Medium	Audit logs were created but not reviewed all of the time. This was found on one of the servers on one network out of 10	< 1%	10 systems
Low	Awareness training was not always competed timely	2% or 10 users	500 users

By using a prioritization, managers will have access to an easier way to allocate resources to problem areas within the field of IT security.

Section 7.5 Utilize Delphi Structured Tools to Facilitate Prioritization

There are already methods available to prioritize findings and concerns of IT security issues. This dissertation proposes a technique, the Ten Step Delphi Security Model, to allow individual findings to be prioritized for implementation. The Ten Step Security Delphi Model is described in Appendix 6: Introduction of the Delphi Process as Part of the Audit Process. This is somewhat different in using a risk assessment methodology, in that it introduces the various stakeholders into the decision-making process. This is significant, where business stakeholders are impacted by costing, additional security requirements, or scheduling concerns. This allows agencies to make business decisions relative to the entire organization, using a structured approach. Stakeholders include any person or group, who may be impacted by the implementation of either a computer application and/or the security controls affecting the computer application. Examples of stakeholders include: business owner of the application; finance office; IT organization providing technology support; or security personnel.

Chapter 8 Recommendations for Future Work

Future work needs to be conducted to enable federal agencies to more successfully evaluate IT security programs. Evaluation techniques are critical to ensure problems and success factors related to IT security are identified. Specific recommendations for future research include:

- Explore the use of management processes and techniques to prioritize IT security work to allow all stakeholders to have input into the IT security requirements
- Determine how findings from IT security audits can be prioritized to allow agencies to focus on most significant problems first
- Determine how statistical sampling methods can be used and integrated into the IT audit process
- The Clinger-Cohen Act of 1996 mandated that Federal Agencies develop and maintain an enterprise IT architecture. The Federal Enterprise Architecture Framework (FEAF) was established in 1999 by the Chief Information Officers (CIO) in response to this mandate. The purpose of the FEAF is to facilitate shared development of common processes and information among Federal Agencies and other government agencies (Popkin, 2005). Another recommendation is to determine how the evaluation and auditing of federal agencies will be impacted with the development of the FEAF.

References

AICIPA. (2004). Government audit quality center: What is a governmental audit? Retrieved May 26, 2005, from http://gaqc.aicpa.org/information+on+Governmental+audits.htm

Bush, G.W. (2002). Expanded electronic government: The president urges agencies to work together on 24 e-gov projects. Retrieved May 26, 2005, from http://www.whitehouse.gov/results/agenda/fiveinitatives04.html

Bush, G.W. (2005). The President's Management Agenda: The scorecard. Retrieved May 26, 2005, from http://www.whitehouse.gov/results/agenda/scorecard.html

Computer Science and Telecommunications Board, National Research Council. (1991). *Computers at risk: Safe computing in the information age*. Washington: National Academy Press.

Computer Science and Telecommunications Board, National Research Council. (2002). *Cybersecurity today and tomorrow: Pay now or pay later*. Washington: National Academy Press.

Computer Research Association (CRA). (2003). CRA Conference on Grand Research Challenges in Information Security & Assurance. Retrieved May 26, 2005, from http://www.cra.org/Activities/grand.challenges/security/home.html

Cooper, D.R. & Schindler, P.S. (2003). *Business research methods*. Boston: McGraw-Hill Irwin.

Creswell, J.W. (1994). *Research design: Qualitative & quantitative approaches*. Thousand Oaks: Sage Publications.

Davis, T. (2005). Federal computer security report card 2004. *Government Reform Committee*. Retrieved May 26, 2005, from http://reform.house.gov/UploadedFiles/2004_Computer_Security_Report_card_2_years.pdf

Delphi Method Home Page. (2004). *Home page for Delphi method/technique/studies in the World Wide Web*. Retrieved May 26, 2005, from http://members.tripod.com/SSM_Delphi/delphi2.htm

Department of Commerce, Office of Communication & Technology. (2003). *A guide for government agencies calculating return on security investment*. Retrieved May 26, 2005, from http://www.oit.nsw.gov.au/content/7.1.15.ROSI_2.asp

Department of Homeland Security. (2005). Homeland security. Retrieved May 26, 2005, from http://www.whitehouse.gov/homeland/

Desmond, P. (2000, September). When security fails: Network forensics can help you recover from a security breach and catch the culprit. *Buzz*. Retrieved May 26, 2005, from http://www.nwfusion.com/buzz2000/buzz- forensics.html

Dorobek, C.J. (2003, September 12). In first security grades, government gets a d-. *Planet.gov*. Retrieved May 26, 2005, from http://www.yensid.net/resume/PlanetGov/20001219ittransition.html

Federal Bureau of Investigation. (2003). Retrieved May 26, 2005, from www.fbi.gov

Federal Computer Incident Response Center. (2002). *Federal information security management act*. Retrieved May 26, 2005, from http://www.gsa.gov/Portal/gsa/ep/contentView.do?pageTypeId=8199&channelId=-13338&P=XAE&contentId=11782&contentType=GSA_BASIC

Federal Trade Commission. (2005). ID theft home: Welcome to the federal trade commission: Your national resource for identity theft. Washington: FTC. Retrieved May 26, 2005, from www.consumer.gov/idtheft

FitzGerald, J. (1999). *Business data communications and networking*. 6th ed. New York: John Wiley & Sons.

Gabor, A. (1990). *The man who discovered quality: How W. Edwards Deming brought the quality revolution to America – the stories of Ford, Xerox, and GM*. New York: Penguin.

Gerstberger, P.G. & Allen, T.J. (1968). Criteria used by research and development engineers in the selection of an information source. *Journal of Applied Psychology*. 52, 4, 272-279.

Gharajedaghi, J. (1999). *System thinking: Managing chaos and complexity: A platform for designing business architecture*. Boston: Butterworth Heinmann.

Goldman, J.E. (1999). *Client/server information systems: A business-oriented approach. 2nd ed*. New York: John Wiley & Sons.

Gomes, L. (2004, January 26). Biggest web problem isn't about privacy it's sloppy security. *Wall Street Journal*. p.B1. Heisenberg, (1927). *Uncertainty paper*. Retrieved May 26, 2005, from http://www.aip.org/history/heisenberg/p08.htm

Information Security. (2004, June). Cover story: First person compliance manager. *Information Security*. Retrieved May 26, 2005, from http://infosecuritymag.techtarget.com/articles/june00/cover_e.shtml

Janis, I.L. (1989). *Crucial decisions*. New York: The Free Press.

Internet Fraud Watch (IFW). (2004). 2001 Internet fraud statistics: Top 10 internet frauds, 2001. Retrieved May 26, 2005, from http://www.fraud.org/internet/intset.htm

Lafourcade, B. & Chapuy, P. (2000). Scenarios and actors' strategies: The case of the agri-foodstuff sector. *Technological Forecasting and Social Change, 65, 67-80 (2000)*. New York: North-Holland.

Laudon, K.C. & Jane P. (2002). *Management information systems*. Upper Saddle River: Prentice Hall.

Lithwicka, D. & Turner, J. (2003, September 8). A guide to the patriot act, part I: Should you be scared of the patriot act? Retrieved May 26, 2005, from http://slate.msn.com/id/2087984/

Mann, C.J. (1995). *Social process analysis: A practical framework and methods for analyzing social change.* College Park. Web Tycho Reserve at University of Maryland University College.

Mark, R. (2004, March 17). Infrastructure: House panel slams federal it security. *Internet.com*. Retrieved May 26, 2005, from www.internetnews.com/infra/article.php/3327081

Microsoft. (2004). Microsoft security. Retrieved May 26, 2005, from http://www.microsoft.com/security/default.mspx

National Institute of Standards and Technology (NIST). (1986). *Privacy act of 1986*. Retrieved May 26, 2005, from http://www.osec.doc.gov/cio/oipr/ITSECDOC1.HTML#Office_of_Management_and_Budget

National Institute of Standards and Technology (NIST). (1994). *Federal information processing standards 91: Specifications for guidelines for the analysis local area network security*. Retrieved May 26, 2005, from http://csrc.nist.gov/publications/fips/fips191/fips191.pdf

National Institute of Standards and Technology (NIST), (1995). *An Introduction to computer security: The NIST handbook*. Retrieved May 26, 2005, from http://csrc.ncsl.nist.gov/publications/nistpubs/800-12/handbook.pdf

National Institute of Standards and Technology (NIST). (2004). Common Criteria: Products in Evaluation. (2004*)*. Retrieved May 26, 2005, from http://niap.nist.gov/ccscheme/in_evaluation.html

National Institute of Standards and Technology (NIST). (2002). Federal computer security program managers forum: IT security metrics workshop. Workshop meeting notes. NIST: Washington.

National Institute of Standards and Technology (NIST). (2004). *FISMA implementation project*. Retrieved May 26, 2005, from http://csrc.nist.gov/sec-cert/

National Institute of Standards and Technology (NIST). (1996, September). *Generally accepted principles and practices for security information technology systems.* NIST Special Publication 800-14. Washington: Government Printing Office.

National Institute of Standards and Technology (NIST). 2003. It security metrics. Retrieved May 26, 2005, from http://www.itl.nist.gov/lab/bulletns/bltnaug03.htm

National Institute of Standards and Technology (NIST). (2004). *Security metrics guide for information technology systems*. Washington: Government Printing Office.

National Institute of Standards and Technology (NIST). (2004). Federal information processing standards. Retrieved May 26, 2005, from http://www.itl.nist.gov/fipspubs/

National Research Council, Computer Science & Telecommunications Board. (1999). *Trust in cyberspace*. Washington: National Academy Press.

National Research Council, Computer Science & Telecommunications Board. (2002). *Information technology research, innovation, and e-government*. Washington: National Academy Press.

National Security Agency. (2004). National security agency: Central security service. Retrieved May 26, 2005, from http://www.nsa.gov/snac/downloads_win2000.cfm?MenuID=scg10.3.1.1

Newman, R.C. (2003). *Enterprise security*. Upper Saddle River: Prentice Hall.

Norusis, M.J. (2002). *SPSS 11.0: Guide to data analysis*. Upper Saddle River: Prentice Hall.

Office of Management and Budget. (2002). *Presidents management agenda*. Retrieved May 26, 2005, from http://www.whitehouse.gov/omb/budget/fy2002/mgmt.pdf

Office of Management and Budget, (2003). *Circular No. A-133 Audits of states, local governments, and non-profit organization.* Retrieved June 27, 2005, from http://www.whitehouse.gov/omb/circulars/a133/a133.html

Office of Management and Budget. (2003, November 3). Management of federal information resources. Retrieved May 26, 2005, from http://www.whitehouse.gov/omb/circulars/a130/appendix_ii.pdf

Office of Management and Budget. (2004). Memorandum for Chief Information Officers: Subject: Expanded electronic government (e-gov) presidents management agenda (pma) scorecard cost, schedule, performance standard for success. Retrieved May 26, 2005, from http://www.whitehouse.gov/omb/memoranda/fy04/m04-24.html

Office of Management and Budget. (2005). Agency scorecards. Retrieved May 26, 2005, from http://www.whitehouse.gov/omb/budintegration/scorecards/agency_scorecards.html

O'Reilly & Associates, Inc. (1992) *Computer security basics*. O'Reilly & Associates: Sebastopol.

Pfleeger, C.P. (1989). *Security in computing*. Englewood Cliffs: Prentice Hall.

Popkin Software. (2005). System architect's mapping to feaf. Enterprise Architecture Company. *Popkin Software*. Retrieved June 27, 2005, from http://government.popkin.com/frameworks/teaf.htm

Putman, A. (2003, December 9). Federal computer security report card: Statement of chairman Putman. Retrieved May 26, 2005, from http://reform.house.gov/TIPRC/News/DocumentSingle.aspx?DocumentID=8889

Putman, A. (2003, March 13). Putman highlights federal e-government initiatives: News release of Congressman Adam Putman, 12th District Florida. Retrieved May 26, 2005, from http://www.adamputnam.house.gov/pressreleases/egovernmentsubcommitteehearing.doc

Putman. (2003, June 24). Cyber security: The status of federal information security and the effects of the "cyber security": The status of federal information security and the effects of the federal information security management act at federal agencies. Retrieved May 26, 2005, from http://reform.house.gov/TIPRC/Hearings/EventSingle.aspx?EventID=7165

Saita, A. (2003, December 12). When a "d" in cybersecurity is seen as an improvement. *Security Wire Perspectives*. Retrieved May 26, 2005, from http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci941114,00.html

Sammon, B. (2002, March 21). Web sites told to delete data. *Washington Times*. Retrieved May 26, 2005, from http://www.mapcruzin.com/news/rtk032202a.htm

Senge, P. (2005, January). Peter Senge and the learning organization. *Infed*. Retrieved May 26, 2005, from http://www.infed.org/thinkers/senge.htm

State of Florida. (2005, January). Auditing in an electronic environment (e-auditing). Retrieved May 26, 2005, from http://www.dor.state.fl.us/dor/taxes/computer_assist.html

Strohm, C. (2003, December). Agencies get failing grades on cybersecurity. *Govexec.com*. Retrieved May 26, 2005, from http://www.govexec.com/dailyfed/1203/120903c1.htm

Robinson, C. (2005). Collecting effective security metrics. Robert Frances Group. Retrieved May 26, 2005, from http://www.csoonline.com/analyst/report2412.html

Tipton, H.F. & Krause, M. (2001*). Information security management handbook*, 4th edition. Boca Raton: Auerbach.

Thomas, D. (2004, September). Information security fails to reach the boardroom. *Computing*. Retrieved May 26, 2005, from http://www.computing.co.uk/news/1158287

Turoff, M. & Hill, S.R. (2004, March 3). Computer based Delphi process. Retrieved May 26, 2005, from http://eies.njit.edu/~turoff/Papers/delphi3.html

United States Department of Defense. (n.d.). *A guide to understanding security testing and test documentation in trusted systems*. (NCSC-TG-023). Fort George G. Meade: National Computer Security Center.

United States Department of Defense. (1983, August 15). *DoD trusted computer system evaluation criteria*. (5200.28-STD). George G. Meade: National Computer Security Center. Retrieved June 27, 2005, from http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html

United States Department of Defense (1985, April 12). *DoD password management guideline. (CSC-STD-002-85).* George G. Meade: National Computer Security Center. Retrieved June 27, 2005, from http://www.radium.ncsc.mil/tpep/library/rainbow/CSC-STD-002-85.html

United States Department of Defense. (1985, June 25). *Computer security requirements: Guidance for applying the dod tcec in specific environments*. (CSC-STD-003-85). George G. Meade: National Computer Security Center. Retrieved June 27, 2005, from http://www.radium.ncsc.mil/tpep/library/rainbow/CSC-STD-003-85.html

United States Department of Defense. (1987). NTISSAM COMPUSEC/1-87. *Advisory memorandum on office automation security guideline.* George G. Meade: National Computer Security Center.

United States Department of Defense, (1987, July 31). *Trusted network interpretation of the trusted computer evaluation criteria*. (NCSC-TG-005). Fort George G. Meade: National Computer Security Center. Retrieved June 27, 2005, from http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-005.html

United States Department of Defense. (1987, September 30). *A guide to understanding discretionary access control in trusted systems*. (NCSC-TG-003). Fort George G. Meade: National Computer Security Center. Retrieved June 27, 2005, from http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-003.html

United States Department of Defense. (1988, October 21). *Glossary of computer security terms*. (NCSC-TG-004). Fort George G. Meade: National Computer Security Center.

United States Department of Defense. (1988, March 28). *A guide to understanding configuration management in trusted systems.* (NCSC-TG-006). Fort George G. Meade: National Computer Security Center.

United States Department of Defense. (1988, September 16).*Computer security subsystem interpretation of the trusted computer system evaluation criteria*. (NCSC-TG-009). Fort George G. Meade: National Computer Security Center. Retrieved June 27, 2005, from http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-003.html

United States Department of Defense. (1988, October 6). *A guide to understanding design documentation in trusted systems*. (NCSC-TG-007). Fort George G. Meade: National Computer Security Center. Retrieved June 27, 2005, from http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-007.html

United States Department of Defense. (1988, December 15). *A guide to understanding trusted distribution in trusted systems*. (NCSC-TG-008). Fort George G. Meade: National Computer Security Center. Retrieved June 27, 2005, from http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-008.html

United States Department of Defense. (1989, April 1). *Guidelines for formal verification systems*. Fort George G. Meade: National Computer Security Center. (NCSC-TG-014). Retrieved June 27, 2005, from http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-014.html

United States Department of Defense. (1989, July 7). *Trusted unix working group (TRUSIX) rationale for selecting access control list features for the unix® system*. (NCSC-TG-020A). Fort George G. Meade: National Computer Security Center. Retrieved June 27, 2005, from http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-020-A.html

United States Department of Defense. (1989, October 18). *A guide to understanding trusted facility management.* (NCSC-TG-015*).* Fort George G. Meade: National Computer Security Center. Retrieved June 27, 2005, from http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-015.html

United States Department of Defense. (1990, June 22). *Trusted product evaluations – a guide for vendors*. (NCSC-TG-002). George G. Meade: National Computer Security Center. Retrieved June 27, 2005, from http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-002.html

United States Department of Defense. (1990, August 1). *Trusted network interpretation environments guideline*. (NCSC-TG-011). Fort George G. Meade: National Computer Security Center. Retrieved June 27, 2005, from http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-011.html

United States Department of Defense. (1991, April). *Trusted database management system interpretation of the t rusted computer system evaluation criteria*. (NCSC-TG-021). Fort George G. Meade: National Computer Security Center.

United States Department of Defense. (1991, September). *A guide to understanding data remanence in Automated Information Systems*, Version 2 (CSC-STD-005-85). Fort George G. Meade: National Computer Security Center.

United States Department of Defense. (1991, September). *A guide to writing the security features user's guide for trusted systems*. (NCSC-TG-026). Fort George G. Meade: National Computer Security Center. Retrieved June 27, 2005, from http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-026.html

United States Department of Defense. (1991, September). *A guide to understanding identification and authentication in trusted systems*. (NCSC-TG-017). Fort George G. Meade: National Computer Security Center. Retrieved June 27, 2005, from http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-017.html

United States Department of Defense. (1991, December). *A guide to understanding trusted recovery in trusted systems*. (NCSC-TG-022). Fort George G. Meade: National Computer Security Center. Retrieved June 27, 2005, from http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-022.html

United States Department of Defense. (1992, May 2). *Trusted product evaluation questionnaire*. (NCSC-TG-019) Version 2. Fort George G. Meade: National Computer Security Center. Retrieved June 27, 2005, from http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-019.2.html

United States Department of Defense. (1992, July). *A guide to understanding object reuse in trusted system*. (NCSC-TG-018). Fort George G. Meade: National Computer Security Center. Retrieved June 27, 2005, from http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-018.html

United States Department of Defense. (1992, October). *A guide to understanding security modeling in trusted systems*. (NCSC-TG-010). Fort George G. Meade: National Computer Security Center.

United States Department of Defense. (1992, October). *Guidelines for writing trusted facility manuals*. (NCSC-TG-016). Fort George G. Meade: National Computer Security Center. Retrieved June 27, 2005, from http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-016.html

United States Department of Defense, (1992, May). *A guide to understanding information system security officer responsibilities for automated information systems*. (NCSC-TG-027). Fort George G. Meade: National Computer Security Center.

United States Department of Defense. (1992, May). *Assessing controlled access protection.* (NCSC-TG-028). Fort George G. Meade: National Computer Security Center.

United States Department of Defense. (1992, December). *A guide to procurement of trusted systems: Computer security contract data requirements list and data item description tutorial: Volume 1 of 4.* (NCSC-G-024 Vol. 1/4). Fort George G. Meade: National Computer Security Center. Retrieved June 27, 2005, from http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-024-1.html

United States Department of Defense. (1993, June). *A guide to procurement of trusted systems: Computer security contract data requirements list and data item description tutorial: Volume 2 of 4*. (NCSC-G-024 Vol. 2/4). Fort George G. Meade: National Computer Security Center.

United States Department of Defense. (1993, November). *A guide to understanding covert channel analysis of trusted systems*. (NCSC-TG-030). Fort George G. Meade: National Computer Security Center.

United States Department of Defense. (1994, January). *Introduction to certification and accreditation concepts*. (NCSC-TG-029). Fort George G. Meade: National Computer Security Center.

United States Department of Defense. (1994, February). *A guide to procurement of trusted systems: Computer security contract data requirements list and data item description tutorial*. (NCSC-TG-024 Vol 3/4). Fort George G. Meade: National Computer Security Center. Retrieved June 27, 2005, from http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-024-3.html

United States Department of Defense. (1995, March 1). RAMP *Program document*. (NCSC-TG-013 Ver 2). Fort George G. Meade: National Computer Security Center. Retrieved June 27, 2005, from http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-013.2.html

United States Department of Defense. (1998, June). *A guide to understanding audit in trusted systems 1*, Version 2. (Tan Book). George G. Meade: National Computer Security Center.

United States Department of Defense. (November 23, 2003). *Trusted product evaluation program*: (5200-28). George G. Meade: National Computer Security Center.

United States General Accounting Office. (1999). *Federal information system controls audit manual, volume 1: Financial statements audits. (*GAO/AIMD-12.19.6). Washington: GAO.

United States General Accounting Office. (March 29, 2000). *Federal information security: Actions needed to address widespread weaknesses: Statement of Jack L. Brock Jr., Director Government Wide and Defense Information Systems.* Washington: GAO.

United States General Accounting Office. (2001). *Information security: Critical infrastructure: Significant challenges in safeguarding information and privately controlled systems from computer-based attacks.* (GAO-01-1168T*)*. Washington: GAO.

United States General Accounting Office. (2001). *Information security: Weak controls place interior's financial and other data at risk*. (GAO-01-615). Washington: GAO.

United States General Accounting Office. (2001). *Information security: Weaknesses place commerce data and operations at serious risk. (*GAO-01-1004T*).* Washington: GAO

United States General Accounting Office. (August, 2001). *Information security: Weaknesses place commerce data and operations at serious risk*. (GAO-01-751T). Washington: GAO. pp. 8, 11, 14-15, 30-32, 38-39.

United States General Accounting Office. (2002). *Child support enforcement: Most states collect drivers' SSNs and use them to enforce child support.* (GAO-02-239). Washington: GAO.

United States General Accounting Office. (2002). *Information security: Corps of engineers making improvements but weaknesses continue*. (GAO-02-589*).* Washington: GAO.

United States General Accounting Office. (March 2002). *Education financial management: Weak internal controls led to instances of fraud and other improper payments.* Washington: GAO. Pp. 1-3.

United States General Accounting Office. (March 2002). *Information security: Additional actions needed to fully implement reform legislation*. Washington: GAO. Pp. 25-28.

United States General Accounting Office. (March, 2002). *International electronic commerce: Definitions and policy implications*. Washington: GAO. P. 1-5.

United States General Accounting Office. (May 1, 2002). *Government purchase cards: Control weaknesses expose agencies to fraud and abuse*. Washington: GAO. P. 3-13.

United States General Accounting Office. (May 2002). *Social security administration: Agency must position itself now to meet profound challenges*. Washington: GAO, p.2, 19-23.

United States General Accounting Office. (2003). *Information security: Progress made but challenges remain to protect federal systems and the nation's critical infrastructures*. (GAO-03-564T). Washington: GAO.

United States General Accounting Office. (November, 2003). *Information security: Improvements needed in treasury security management program*. Washington: GAO.

United States General Accounting Office. (2004). *Information security: Further efforts needed to address serious weaknesses at USDA*. (GAO-04-154*).* Washington: GAO.

United States General Accounting Office. (2004). *Special publications: Computers and information technology*. Retrieved May 26, 2005, from http://www.gao.gov/special.pubs/cit.html

United States General Accounting Office. (March, 2004). *Information security: Continued efforts needed to sustain progress in implementing statutory requirements*. Washington: GAO. P.1.

United States Government Accountability Office. (November 29, 2004). *Meeting conducted at GAO between Ellen Pieklo & GAO personnel to discuss concept paper*. Washington: GAO Building.

United States Government Accountability Office. (January , 2005). *About GAO reports: How do GAO studies get their start*. Retrieved May 26, 2005, from http://www.gao.gov/about/aboutrpt.html

United States Government Accountability Office. (January 5, 2005). *Email message sent from GAO to Ellen Pieklo*.

Volpe, J. (2003). Risk assessment and prioritization. *Volpe Journal*. p. 4-6.

Appendices

Appendix 1	**contains key definitions of the word system and the illustration of misuse of terminology**
Appendix 2	**contains GAO Reports and Associated Findings**
Appendix 3	**contains feedback from the presentation of the concept paper to GAO**
Appendix 4	**contains the Delphi Ten Step Security model**
Appendix 5	**contains the GAO PowerPoint presentation**

Appendices: Table of Contents

Appendix 1

Key: Definitions of the word "system" within 1 GAO report

Enterprise System = Entire concept of networks, operating systems, entire application and system concepts

Network/OS = Discussion of system, in which both the operating system and network are included

Network Controls = Point at which the network can be compromised, such as with routers and firewalls

Operating System = Controls specific to the machine for an operating system

Application = Defined as part of the application controls or an application program

Roles = Roles played by a user, manager, or operator of the system

Business Process = Specific application residing in an agency's environment

Unclear = Not clear what context the word system is being used

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
1	I am pleased to be here to discuss our analysis of the information security controls over unclassified ***systems*** of the Department of Commerce (Commerce).	1	• Unclassified systems	Enterprise System
1	However, along with the enormous benefits it brings, this	1	• Computer systems	Network/OS

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	widespread interconnectivity poses significant risks to our computer ***systems***, and more important, to the critical operations and infrastructures they support.			
1	As with other organizations, Commerce relies extensively on computerized ***systems*** and electronic data to support its mission.	1	• Computerized systems	Network/OS
1	Accordingly, the security of its ***systems*** and data is essential to avoiding disruption in critical operations, data tampering, fraud, and inappropriate disclosure of sensitive information.	1	• Security of its systems	Unclear
1	Further, there has been a dramatic rise in the number and sophistication of cyber attacks on federal ***systems***.	1	• Federal systems	Network Controls
1	My testimony today specifically focuses on the effectiveness of Commerce's (1) Logical access controls	1	• Information system controls	Unclear

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	And other information ***system*** controls over its computerized data, (2) incident detection and response capabilities and (3) information security management program and related procedures.			
2	At the seven Commerce organizations we reviewed, significant and pervasive computer security weaknesses exist that place sensitive Commerce ***systems*** at serious risk.	1	• Sensitive Commerce systems	Enterprise System
2	Using readily available software and common techniques, we demonstrated the ability to penetrate sensitive Commerce ***systems*** from both inside Commerce and remotely, such as through the Internet.	1	• Sensitive Commerce systems	Network/OS
2	Using readily available software and common techniques, we demonstrated the ability to penetrate	2	• Sensitive Commerce system	Enterprise System

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	Sensitive Commerce ***systems*** from both inside Commerce and remotely, such as through the Internet. Individuals, both within and outside Commerce, could gain unauthorized access to these ***systems*** and read, copy, modify, and delete sensitive economic, financial, personnel, and confidential Business data.		• Unauthorized access to these systems	Operating System
2	Moreover, intruders could disrupt the operations of ***systems*** that are critical to the mission of the department.	1	• Operations of systems	Applications
2	Additionally, unauthorized access to sensitive ***systems*** may not be detected in time to prevent or minimize damage.	1	• Unauthorized access to sensitive systems	Network/OS
2	First, controls intended to protect information ***systems*** and critical data from unauthorized access are ineffectively implemented, leaving sensitive ***systems***	2	• Information systems • Sensitive systems highly susceptible to	Enterprise System Enterprise System

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	highly susceptible to intrusions or disruptions.		Intrusions or disruptions	
2	***Systems*** were either not configured to require passwords—including powerful *systems* administrator accounts—or, if passwords were required, they were relatively easy to guess, such as the word "password" or commonly known default passwords supplied by vendors.	2	• Systems were either not configured • Systems administrator accounts	Operating System Roles
2	Further, (1) a significant number of passwords never expired, (2) individuals had unlimited attempts to guess passwords, and (3) unencrypted passwords, including those having powerful ***system*** administrator functions, could be widely viewed.	1	• System administrator functions	Roles
2	Commerce bureaus also granted excessive ***system***	2	• System administration	Roles

Page #	This illustrates sentences using the word “system” and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	administration privileges to employees who did not require them, including 20 individuals who had powerful ***system*** *privileges* that should be used only in exceptional circumstances, such as recovery from a power failure.		Privileges • System privileges	Roles
2 (Footnote)	By “sensitive" ***systems*** we refer to the *systems* that Commerce has defined as critical to the mission of the Department as well as ***system****s* that fit OMB Circular A-130, Appendix III, criteria for requiring special protection	3	• By “sensitive" systems we refer • To the systems that Commerce has defined as critical to the mission of the Department • As well as systems that fit OMB Circular A-130, Appendix III,	Application Enterprise System

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
			Criteria for requiring special protection	
3	The configuration of Commerce operating ***systems*** exposed excessive amounts of ***system*** information to anyone, without the need for authentication, allowing potential attackers to collect ***systems*** information that could be used to circumvent security controls and gain unauthorized access.	3	• Commerce operating systems • Excessive amounts of system information • Collect systems information	Enterprise System Unclear Operating System
3	In addition, Commerce did not properly configure operating ***systems*** to ensure that they would be available to support bureau missions or prevent the corruption of important data.	1	• Operating systems	Operating System
3	For example, in a large computer ***system*** affecting several bureaus, thousands of important programs had not been	2	• Large computer system	Operating system Network/OS

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	assigned unique names, which could result in unintended programs being inadvertently run, potentially corrupting data or disrupting ***system*** operations.		• Disrupting system operations	
3	In this *same* ***system***, because critical parts of the operating ***system*** were shared by the test and production ***system****s*, changes in either ***system*** could corrupt or shut down the other *system.*	5	• Same system • Critical parts of the operating system • Test and production systems • Changes in either system • Corrupt or shut down the other system	Unclear Operating System Applications Operating System Operating System
3	Additionally, unnecessary and poorly configured ***system*** functions existed on important computer ***system****s* in all	2	• Unnecessary and poorly configured	Network/OS

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	bureaus we reviewed, allowing us to gain access from the Internet.		System functions • Important computer systems	Unclear
3	Our testing demonstrated that individuals, both within and outside Commerce, could compromise external and internal security controls to gain extensive unauthorized access to the department's networks and ***systems***.	1	• Department's networks and systems	Network/OS
3	During our testing we discovered 20 ***systems*** with known vulnerabilities for which patches were available but not installed.	1	• Systems with known vulnerabilities for which patches were available but not installed	Operating System
3	As a result of ineffective detection capabilities, the tested bureaus were generally unable to detect our extensive	1	• Intrusion detection systems	Network Controls

Page #	This illustrates sentences using the word “system” and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	intrusion activities (only two of the bureaus had installed intrusion detection ***systems***).			
3-4	Also, only one of the bureaus has established incident response procedures; in two of five instances when our activity was detected, Commerce employees who detected our testing inappropriately responded by launching attacks against our ***systems***.	1	• Responded by launching attacks against our systems	Unclear
4	This lack of a centralized approach to managing security is particularly risky considering the widespread interconnectivity of Commerce's ***systems***.	1	• Interconnectivity of Commerce's systems	Unclear
4	Commerce is doing little to understand and manage risks to its ***systems***.	1	• Risks to its systems	Enterprise System
4	For example, as of March 2001, of the bureaus' 94 sensitive ***systems*** we reviewed, 91 did not have	1	• Bureaus' 94 sensitive systems	Enterprise System

Page #	This illustrates sentences using the word “system” and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	Documented risk assessments, 87 had no security plans, and none were authorized for processing by Commerce management.			
4	Consequently, most of the bureaus' ***systems*** are being operated without considering the risks associated with their immediate environment.	1	• Bureaus' systems are being operated without considering the risks	Enterprise System
4	Moreover, several bureau officials acknowledged that they had not considered how vulnerabilities in ***systems*** that interconnected with theirs could undermine the security of their own ***system****s*.	2	• Vulnerabilities in systems • Vulnerabilities in *systems* that interconnected with theirs could undermine the security	Network/OS Operating System

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
			Of their own systems	
4	Moreover, Commerce has not updated its policy to reflect the risks of Internet use and has no policies establishing baseline *security requirements for all **system**s*.	1	• Baseline security requirements for all systems	Network/OS
4	Authorization is the acceptance of risk by management, resulting in a formal approval for the ***system*** to become operational or remain so after significant ***system*** changes have been made.	2	• Formal approval for the system • Significant system changes	Enterprise System Unclear
5	Although each of the seven bureaus reviewed have informal programs in place, none have documented computer security training procedures that meet federal requirements for ensuring that security risks and responsibilities are understood by all managers, users, and ***system*** administrators.	1	• System administrators	Roles

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
5	No oversight reviews of the Commerce bureaus' *systems* have been performed by the staff of Commerce's information security program.	1	• Oversight reviews of the Commerce bureaus' systems	Enterprise System
5	Only one of the bureaus has performed isolated tests of its *systems.*	1	• Isolated tests of its systems	Unclear
5	The lack of an effective information security program is exacerbated by Commerce's highly interconnected computing environment in which the vulnerabilities of individual ***systems*** affect the security of ***systems*** in the entire department.	2	• Vulnerabilities of individual systems • Security of systems in the entire department	Network/OS Operating System
5	A compromise in a single poorly secured ***system*** can undermine the security of the multiple ***systems*** that connect to it.	2	• Compromise in a single poorly secured system • Security of the	Operating System Operating System

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
			Multiple systems	
5	Information security is an important consideration for any organization that depends on information ***systems*** to carry out its mission.	1	• Information systems to carry out its mission	Enterprise System
6	Without proper safeguards, these developments make it easier for individuals and groups with malicious intentions to gain unauthorized access to ***systems*** and use their access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other organizations' sites.	1	• Unauthorized access to systems	Operating System
6	Government officials are increasingly concerned about federal computer ***systems***, which process, store, and transmit enormous amounts of sensitive data and are indispensable to many federal operations.	1	• Federal computer systems, which process, store, and transmit enormous	Enterprise System

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
			Amounts of sensitive data and are indispensable to many federal operations	
6	The federal government's ***systems*** are riddled with weaknesses that continue to put critical operations at risk. Since October 1998, the Federal Computer Incident Response Center's (FedCIRC) 9 records have shown an increasing trend in the number of attacks targeting government ***systems***.	2	• Federal government's systems • Attacks targeting government systems	Enterprise System Network Controls
6	In 1998 FedCIRC documented 376 incidents affecting 2,732 federal civilian ***systems*** and 86 military ***systems***	2	• Civilian systems • Military systems	Unclear Unclear
6	In 2000, the number of attacks rose to 586 incidents affecting 575,568 federal ***systems*** and 148 of their	1	• 586 incidents affecting 575,568 federal	Network Controls

Page #	This illustrates sentences using the word “system” and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	military counterparts.		Systems	
Footnote	The term "script kiddie" is used within the hacker community in a derogatory manner to refer to a hacker with little computer knowledge and few abilities who breaks into ***systems*** using scripts posted to the Internet by more skilled hackers.	1	• Breaks into systems using scripts	Operating System
Footnote	FedCIRC, a component of the General Service Administration's Technology Service, is the central coordinating activity for reporting security related incidents affecting computer ***systems*** within the federal government's civilian agencies and departments.	1	• Computer systems within the federal government's civilian agencies and departments	Network/OS
7	In January 2000, President Clinton issued a National Plan for Information ***Systems*** Protection and designated computer security and critical infrastructure protection a	1	• National Plan for Information Systems Protection	Enterprise System

Page #	This illustrates sentences using the word “system” and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	priority management objective in his fiscal year 2001 budget.			
7	These provisions seek to ensure proper management and security for federal information ***systems*** by calling for agencies to adopt risk management practices that are consistent with those summarized in our 1998 Executive Guide.	1	• Federal information systems	Enterprise System
7	The federal CIO Council and others have also initiated several projects that are intended to promote and support security improvements to federal information ***system***s.	1	• Security improvements to federal information systems	Enterprise System
Footnote	A "root compromise" of a ***system*** gives the hacker the power to do anything that a ***systems*** administrator could do, from copying files to installing software such as	2	• "Root compromise" of a system • Systems administrator	Operating System

Page #	This illustrates sentences using the word “system” and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	"sniffer" programs that can monitor the activities of end users.			
7	Defending America’s Cyberspace: National Plan for Information ***Systems*** Protection: An Invitation to a Dialogue.	1	• National Plan for Information Systems Protection	Enterprise System
8	Since 1996, our analyses of information security at major federal agencies have shown that ***systems*** are not being adequately protected.	1	• Systems are not being adequately protected	Operating System
8	Our most recent summary analysis of federal information ***systems*** found that significant computer security weaknesses had been identified in 24 of the largest federal agencies, including Commerce.16	1	• Summary analysis of federal information systems	Enterprise System
8	The department spends significant resources—reportedly over $1.5 billion in fiscal year 2000—on IT ***systems*** and	1	• IT systems and services	Unclear

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	services.			
9	Sensitive data such as that relating to national security, nuclear proliferation, missile technology, and chemical and biological warfare reside in this bureau's ***Systems***.	1	• Sensitive data such as that relating to national security, nuclear proliferation, missile technology, and chemical and biological warfare reside in this bureau's Systems	Operating System
9	For example, export data residing in the BXA ***systems*** reflect technologies that have both civil and military applications; the misuse, modification, or deletion	1	• Export data residing in the BXA system	Application
10	For example, Commerce has 14 different data centers,	1	• Independently	Application

Page #	This illustrates sentences using the word “system” and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	diverse hardware platforms and software environments, and 20 independently managed e-mail **systems**.		Managed e-mail systems	
10	Recognizing the importance of its data and operations, in September 1993 Commerce established department wide information security policies that defined and assigned a full set of security responsibilities, ranging from the department level down to individual ***system*** owners and users within the bureaus.	1	• System owners	Enterprise System
10	The CIO’s responsibilities for the security of classified ***systems*** has been delegated to the Office of Security.	1	• Security of classified systems	Unclear
11	After a 1999 contracted evaluation of the bureaus' security plans determined that 43 percent of Commerce's most critical assets did not have current information ***system*** security plans, the CIO issued a memorandum	1	• Information system security plans	Enterprise System

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	calling for the bureaus to prepare security plans that comply with federal regulations			
11	A basic management objective for any organization is the protection of its information ***systems*** and critical data from unauthorized access.	1	• Information systems	Enterprise System
11	Organizations accomplish this objective by establishing controls that limit access to only authorized users, effectively configuring their operating ***systems***, and securely implementing networks.	1	• Operating systems	Operating System
11	We demonstrated that individuals, both external and internal to Commerce, could compromise security controls to again extensive unauthorized access to commerce networks and ***systems***.	1	• Commerce networks and systems	Network/OS
11	These weaknesses place the bureaus' information ***systems***	1	• Bureaus' information	Enterprise System

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	at risk of unauthorized access, which could lead to the improper disclosure, modification, or deletion of sensitive information and the disruption of critical operations.		Systems at risk of unauthorized access	
12	Effective ***system*** access controls provide mechanisms that require users to identify themselves and authenticate19 their identity, limit the use of ***system*** administrator capabilities to authorized individuals, and protect sensitive ***system*** and data files	3	• Effective system access controls • System administrator capabilities • Protect sensitive system and data files	Operating System Roles Application
12	Commerce's primary means of authenticating user identity. Because ***system*** administrator capabilities provide the ability to read, modify, or delete any data or files on the ***system*** and modify the operating ***system*** to	5	• System administrator capabilities • Provide the ability to read, modify, or delete	Roles Operating System

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	create access paths into the **system**, such capabilities should be limited to the minimum access levels necessary for **system**s personnel to perform their duties.		Any data or files on the system • Create access paths into the system • Modify the operating system • Necessary for systems personnel	Roles Operating System Operating System
12	Also, information can be protected by using controls that limit an individual's ability to read, modify, or delete information stored in sensitive ***system*** files.	1	• Sensitive system files	Operating System
12	One of the primary methods to prevent unauthorized access to information ***system*** resources is through effective management of user IDs and passwords.	1	• To information system resources	Operating System

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
12	All Commerce bureaus reviewed were not effectively managing user IDs and passwords to sufficiently reduce the risk that intruders could gain unauthorized access to its information ***systems*** to (1) change ***system*** access and other rules, (2) potentially read, modify, and delete or redirect network traffic, and (3) read, modify, and delete sensitive information.	2	• Gain unauthorized access to its information systems • Change system access	Network/OS Roles
12	Specifically, *systems* were either not configured to require passwords or, if passwords were required, they were relatively easy to guess.	1	• Systems were either not configured to require passwords	Operating System
12	For example, powerful ***system*** administrator accounts did not require passwords, allowing anyone who could connect to certain ***systems*** through the network to log on as a ***system*** administrator without having to use a	3	• System administrator accounts • System administrator • Allowed to access a	Roles Roles Operating System

Page #	This illustrates sentences using the word “system” and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	password, 19 Authenticating is the process of verifying that a user is allowed to access a ***system*** or an account.		System or an account	
13	***Systems*** allowed users to change their passwords to a blank password, completely circumventing the password control function, passwords were easily guessed words, such as "password," passwords were the same as the user's ID, and commonly known default passwords set by vendors when ***systems*** were originally shipped had never been changed.	2	• Systems allowed users to change their passwords to a blank password • Passwords set by vendors when systems were originally shipped	Operating System Operating System
13	Although frequent password changes reduce the risk of continued unauthorized use of a compromised password, ***systems*** in four of the bureaus reviewed had a significant number of passwords that never required changing or did	1	• Systems in four of the bureaus reviewed had a significant number of passwords	Enterprise System

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	not have to be changed for 273 years.			
13	Also, ***systems*** in six of the seven bureaus did not limit the number of times an individual could try to log on to a user ID.	1	• Systems in six of the seven bureaus	Operating System
13	Further, all Commerce bureaus reviewed did not adequately protect the passwords of their ***system*** users through measures such as encryption, as illustrated by the following examples: - User passwords were stored in readable text files that could be viewed by all users on one bureau's ***systems***. - Files that store user passwords were not protected from being copied by intruders, who could then take the copied password files and decrypt user passwords. The decrypted passwords could then be used to gain	3	• Did not adequately protect the passwords of their system users • Could be viewed by all users on one bureau's systems • Gain unauthorized access to systems	Roles Enterprise system Operating System

Page #	This illustrates sentences using the word “system” and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	unauthorized access to ***systems*** by intruders masquerading as legitimate users.			
13	Unlimited attempts allow intruders to keep trying passwords until a correct password is discovered. - Over 150 users of one ***system*** could read the unencrypted password of a powerful ***system*** administrator's account.	2	• Over 150 users of one system • Powerful system administrator's account	Unclear Roles
13	*System* administrators perform important functions in support of the operations of computer ***systems***.	2	• System administrators • Operations of computer systems	Roles Operating System
13	These functions include defining security controls, granting users access privileges, changing operating ***system*** configurations, and monitoring ***system*** activity. In order to perform these functions, *system* administrators	4	• Changing operating system configurations • Monitoring system activity	Operating System Unclear

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	have powerful privileges that enable them to manipulate operating **system** and security controls.		• System administrators	Roles
13-14	Privileges to perform these ***system*** administration functions should be granted only to employees who require such privileges to perform their responsibilities and who are specifically trained to understand and exercise those privileges.	1	• Privileges to perform these system administration functions	Roles
14	Finally, ***system***s should provide accountability for the actions of ***system*** administrators on the ***systems***.	3	• Systems should provide accountability for the • Actions of system administrators • On the systems	Unclear Roles Unclear

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
14	However, Commerce bureaus granted the use of excessive ***system*** administration privileges to employees who did not require such privileges to perform their responsibilities and who were not trained to exercise them.	1	• Excessive system administration privileges	Roles
14	For example, a very powerful ***system*** administration privilege that should be used only in exceptional circumstances, such as recovery from a power failure, was granted to 20 individuals.	1	• System administration privilege	Roles
14	These 20 individuals had the ability to access all of the information stored on the ***system***, change important ***system*** configurations that could affect the ***system's*** reliability, and run any program on the computer.	3	• 20 individuals had the ability to access all of the information stored on the system • Change important	Operating System Operating System

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
			System configurations • Could affect the system's reliability	Operating System
14	On other important ***systems*** in all seven bureaus, ***system*** administrators were sharing user IDs and passwords so that *systems* could not provide an audit trail of access by *system* administrators, thereby limiting accountability.	3	• On other important systems in all seven bureaus • System administrators • Systems could not provide an audit trail access by system administrators	Enterprise System Operating System Roles
14	By not effectively controlling the number of staff who exercise ***system*** administrator privileges, restricting the level of such privileges granted to those required to	1	• Number of staff who exercise system administrator	Roles

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	perform assigned duties, or ensuring that only well-trained staff have these privileges, Commerce is increasing the risk that unauthorized activity could occur and the security of sensitive information be compromised.		Privileges	
14	Access privileges to individual critical *systems* and sensitive data files should be restricted to authorized users.	1	• Systems and sensitive data files	Application
14	Not only does this restriction protect files that may contain sensitive information from unauthorized access, but it also provides another layer of protection against intruders who may have successfully penetrated one *system* from significantly extending their unauthorized access and activities to other ***systems***.	2	• Provides another layer of protection against intruders who may have successfully penetrated one system • From significantly	Network/OS Network/OS

Page #	This illustrates sentences using the word “system” and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
			Extending their unauthorized access and activities to other systems	
14	Examples of access privileges are the capabilities to read, modify, or delete a file. Privileges can be granted to individual users, to groups of users, or to everyone who accesses the ***system***.	1	• Privileges can be granted to individual users, to groups of users, or to everyone who accesses the system	Operating System
14	Six of the seven bureaus' ***systems*** were not configured to appropriately restrict access to sensitive *system* and/or data files.	1	• Six of the seven bureaus' systems were not configured	Unclear
14-15	For example, critical *system* files could be modified by	1	• Critical system files	Operating System

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	All users to allow them to bypass security controls.		Could be modified by all users	
15	*Systems* configured with excessive file access privileges are extremely vulnerable to compromise because such configurations could enable an intruder to read, modify, or delete sensitive *system* and data files, or to disrupt the availability and integrity of the ***system***.	2	• Systems configured with excessive file access privileges are extremely vulnerable • Configurations could enable an intruder to read, modify, or delete sensitive system and data files, or to disrupt the availability and integrity of the system	Operating System Operating System
15	Operating ***system*** controls are essential to ensure that the	2	• Operating system	Operating System

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	Computer ***systems*** and security controls function as intended.		Controls are essential • To ensure that the computer systems and security controls function as intended	Operating System
15	Operating System are relied on by all the software and hardware in a computer ***system***. Additionally, all users depend on the proper operation of the operating ***system*** to provide a consistent and reliable processing environment, which is essential to the availability and reliability of the information stored and processed by the ***system***.	4	• Operating System are relied on by all the software and hardware • Software and hardware in a computer system • Operation of the operating system to provide a consistent	Operating System Operating System Operating System

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
			And reliable processing environment • Essential to the availability and reliability of the information stored and processed by the system	Operating System
15	Operating ***system*** controls should limit the extent of information that ***systems*** provide to facilitate *system* interconnectivity.	2	• Operating system controls should • Limit the extent of information that systems provide	Operating System Operating System

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
			• To facilitate system interconnectivity	Network Controls
15	Operating System should be configured to help ensure that ***systems*** are available and that information stored and processed is not corrupted.	1	• Operating System should be configured • To help ensure that systems are available and that information stored and processed is not corrupted	Operating System Operating System
15	Access to Critical ***Systems*** and Sensitive Data Files Was Not Adequately Restricted of the computer ***system*** to prevent insecure *system* configurations or the existence of functions not needed to support the operations of the ***system***.	4	• Critical system • Computer system • System configurations • System operations	Application Operating System Operating System Application

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
15	To facilitate interconnectivity between computer ***systems***, operating *systems* are configured to provide descriptive and technical information, such as version numbers and *system* names, to other computer ***systems*** and individuals when connections are being established.	4	• Interconnectivity between computer systems • Operating systems are configured • System names • To other computer systems and individuals when connections are being established	Network Controls Operating System Operating System Operating System
15	At the same time, however, ***systems*** should be configured to limit the amount of information that is made available to other ***systems*** and unidentified individuals because this	2	• Systems should be configured • Limit the amount of	Operating System Operating System/

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	Information can be misused by potential intruders to learn the characteristics and vulnerabilities of that *system* to assist in intrusions.		Information that is made available to other systems • Characteristics and vulnerabilities of that system	Network/OS Operating System
15	Operating ***system*** functions are capabilities added to the operating ***system*** to support specific processing requirements necessary for the ***system*** to perform its intended purpose		• Operating system functions are capabilities added to the operating system • To support specific processing requirements necessary for the	Operating System Operating System

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
			System to perform its intended purpose	
15	Examples of operating ***system*** functions include the capability to receive electronic mail, the capability have technical support performed remotely, the capability to transfer data between different types of computer ***systems,*** and the capability to have users safely execute powerful programs without granting those users powerful access privileges.	2	• Examples of operating system functions the capability to receive electronic mail t • The capability to transfer data between different types of computer systems, and the capability to have users safely execute powerful programs without granting those	Application Operating System/ Network Controls

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
			Users powerful access privileges	
16	***Systems*** in all bureaus reviewed were not configured to control excessive ***system*** information from exposure to potential attackers.	2	• *Systems* in all bureaus reviewed were not configured • To control excessive system information from exposure to potential attackers	Enterprise System Unclear
16	The configuration of Commerce ***systems*** provided excessive amounts of information to anyone, including external users, without the need for authentication.	1	• Configuration of Commerce systems	Enterprise System
16	Our testing demonstrated that potential attackers could collect information about ***systems***, such as computer	2	• Attackers could collect information	Operating System

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	names, types of operating ***systems***, functions, version numbers, user information, and other information that could be useful to circumvent security controls and gain unauthorized access.		about systems • Types of operating systems	Operating System
16	The proper configuration of operating ***systems*** is important to ensuring the reliable operation of computers and the continuous availability and integrity of critical information.	1	• Proper configuration of operating systems is important	Operating System
16	Operating System should be configured so that the security controls throughout the ***system*** function effectively and the ***system*** can be depended on to support the organization's mission.	3	• Operating System should be configured so that the • Security controls throughout the system function effectively	Operating System Operating System

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
			• And the system can be depended on to support the organization's mission	Operating System
16	Commerce bureaus did not properly configure operating ***systems*** to ensure that ***systems*** would be available to support bureau missions or prevent the corruption of the information relied on by management and the public	2	• Commerce bureaus did not properly configure operating systems • To ensure that systems would be available to support bureau missions	Operating System Enterprise System
16	For example, in a large computer ***system*** affecting several bureaus, there were thousands of important programs that	1	• For example, in a large computer system	Operating System

Page #	This illustrates sentences using the word “system” and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	had not been assigned unique names. In some instances, as many as six different programs all shared the same name, many of which were different versions of the same program.		Affecting several bureaus	
16	Although typically the complexity of such a ***system*** may require the installation of some programs that are identically named and authorized programs must be able to bypass security in order to operate, there were an excessive number of such programs installed on this ***system***, many of which were capable of bypassing security controls.	2	• Typically the complexity of such a system may require the installation of some programs that are identically named and authorized • There were an excessive number of such programs	Operating System Operating System

Page #	This illustrates sentences using the word “system” and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
			Installed on this system, many of which were capable of bypassing security controls.	
16	Because these different programs are identically named, unintended programs could be inadvertently run, potentially resulting in the corruption of data or disruption of ***system*** operations.	1	• Disruption of system operations	Business process
16	In this same ***system***, critical parts of the operating ***system*** were shared by the test and production ***systems*** used to process U.S. export information.	3	• In this same system • Critical parts of the operating system were shared • By the test and	Operating System Operating System Operating System

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
			Production systems used to process U.S. export information	
16	Because critical parts were shared, as changes are made in the test ***system***, these changes could also affect the production ***system***.	2	• Test system • Production system	Operating System Operating System
16	Consequently, changes could be made in the test ***system*** that would cause the production ***system*** to stop operating normally and shut down.	2	• Test system • Production system	Operating System Operating System
	Changes in the test ***system*** could also cause important Commerce data in the production ***system*** to become corrupted.	2	• Test system • Production System	Operating System Operating System
16 -17	Commerce management acknowledged that the isolation between these two ***systems*** needed to be strengthened to	1	• Isolation between these two systems	Operating System

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	Mitigate these risks.		Needed to be strengthened	
17	Operating *system* functions should be limited to support only the capabilities needed by each specific computer ***system***.	2	• Operating system functions should be limited • Support only the capabilities needed by each specific computer system	Operating System Operating System
17	Unnecessary operating ***system*** functions can be used to gain unauthorized access to a ***system*** and target that ***system*** for a denial-of-service attack.	3	• Unnecessary operating system functions can be used to gain unauthorized access • Unauthorized access	Network/OS Operating System

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
			To a system • Target that system for a denial-of-service attack	Network/OS
17	Poorly configured operating ***system*** functions can allow individuals to bypass security controls and access sensitive information without requiring proper identification and authentication.	1	• Poorly configured operating system functions	Operating System
17	Unnecessary and poorly configured ***system*** functions existed on important computer ***systems*** in all the bureaus we reviewed.	2	• Unnecessary and poorly configured system functions existed on important • Computer systems	Operating System Operating System
17	For example, unnecessary functions allowed us to gain	4	• Unnecessary functions	Network/OS

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	Access to a ***system*** from the Internet. Through such access and other identified weaknesses, we were able to gain ***system*** administration privileges on that ***system*** and subsequently gain access to other ***systems*** within other Commerce bureaus.		Allowed us to gain access to a system from the Internet • We were able to gain system administration privileges • On that system and subsequently • Gain access to other systems	Roles Operating System Network/OS
17	Networks are a series of interconnected information technology devices and software that allow groups of individuals to share data, printers, communications ***systems,*** electronic mail, and other resources.	1	• Allow groups of individuals to share data, printers, communications	Network Controls

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
			Systems, electronic mail, and other resources	
17	Controls should also limit the use of ***systems*** from sources internal to the network to authorized users for authorized purposes.	1	• Controls should also limit the use of systems from sources internal to the network	Unclear
Footnote	The second type of attack overloads some ***system*** service or exhausts some resource, thus preventing others from using that service.	1	• The second type of attack overloads some system service or exhausts some resource	Network/OS
18	External threats can be countered by implementing security controls on the perimeters of the network, such	2	• That limit user access and data interchange	Network Controls

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	as firewalls, that limit user access and data interchange between **systems** and users within the organization's network and ***systems*** and users outside the network, especially on the Internet.		Between systems and users • Within the organization's network and systems and users outside the network	Network/OS
18	An example of perimeter defenses is only allowing pre-approved computer ***systems*** from outside the network to exchange certain types of data with computer ***systems*** inside the network.	2	• Allowing pre-approved computer systems • Computer systems inside the network	Network/OS
18	External network controls should guard the perimeter of the network from connections with other *systems* and	1	• Connections with other systems	Network Controls

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	access by individuals who are not authorized to connect with and use the network.			
18	Also, an intruder who has successfully penetrated a network's perimeter defenses becomes an internal threat when the intruder attempts to compromise other parts of an organization's network security as a result of gaining access to one *system* within the network.	1	• Gaining access to one system within the network	Network/OS
18	For example, at Commerce, users of one bureau who have no business need to access export license information on another bureau's network should not have had network connections to that *system*.	1	• Network connections to that system	Network Controls
18	External network security controls should prevent unauthorized access from outside threats, but if those controls fail, internal network security controls should	1	• Unauthorized access to other computer systems within the	Network/OS

Page #	This illustrates sentences using the word “system” and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	also prevent the intruder from gaining unauthorized access to other computer *systems* within the network.		Network	
18	Individuals, both within and outside Commerce, could compromise external and internal security controls to gain extensive unauthorized access to Commerce networks and *systems*.	1	• Gain extensive unauthorized access to Commerce networks and systems	Enterprise System
Footnote	Firewalls are hardware and software components that protect one set of *system* resources (e.g., computers and networks) from attack by outside network users (e.g., Internet users) by blocking and checking all incoming network traffic. Firewalls permit authorized users to access and transmit privileged information and deny access to unauthorized users.	1	• Protect one set of system resource	Network/OS
19	For example, four bureaus had not configured their	1	• Information system	Enterprise System

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	firewalls to adequately protect their information *systems* from intruders on the Internet.			
19	Weaknesses in the external and internal network controls of the individual bureaus heighten the risk that outside intruders with no prior knowledge of bureau user IDs or passwords, as well as Commerce employees with malicious intent, could exploit the other security weaknesses in access and operating *system* controls discussed above to misuse, improperly disclose, or destroy sensitive information.	1	• Operating system controls	Operating System
19-20	These information *system* controls include policies, procedures, and techniques to provide appropriate segregation of duties among computer personnel, prevent unauthorized changes to application programs, and	1	• Information System controls	Unclear

Page #	This illustrates sentences using the word “system” and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	ensure the continuation of computer processing operations in case of unexpected interruption.			
20	These two functions are not compatible since the individual's familiarity with *system* security could then allow him or her to bypass security controls either to facilitate performing administrative duties or for malicious purposes.	1	• System security	Unclear
21	Specific key controls not addressed were (1) operating *system* software changes, monitoring, and access and (2) controls over application software libraries including access to code, movement of software programs, and inventories of software.	1	• Operating system	Operating System
21	Only three of the seven bureaus we reviewed mentioned software change controls in their *system* security plans,	1	• System security plans	Enterprise System

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	while none of the bureaus had policies or procedures for controlling the installation of software.			
21	Such policies are important in order to ensure that software changes do not adversely affect operations or the integrity of the data on the *system*.	1	• Data on the system	Operating System
21	Such a plan is critical for helping to ensure that information *system* operations and data can be promptly restored in the event of a service disruption.	1	• System operations	Business process
22	None of the seven bureaus had completed recovery plans for all of their sensitive *systems*.	1	• Sensitive systems	Enterprise System
22	Although one bureau had developed two recovery plans, one for its data center and another for its software development installation center, the bureau did not have plans to cover disruptions to the rest of its critical	1	• Critical systems	Application Network/OS

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	systems, including its local area network.			
22	*Systems* at six of the seven bureaus did not have documented backup procedures.	1	• Systems of six of the seven bureaus	Enterprise System
22	One bureau stated in its backup strategy that tapes used for *system* recovery are neither stored off-site nor protected from destruction.	1	• System recovery	Network/OS
22	Until each of the Commerce bureaus develops and fully tests comprehensive recovery plans for all of its sensitive *systems*, there is little assurance that in the event of service interruptions, many functions of the organization will not effectively cease and critical data will be lost.	1	• Recovery plan for systems	Network/OS
22	As our government becomes increasingly dependent on information *systems* to support sensitive data and mission critical operations, it is essential that agencies protect	1	• Information systems	Enterprise System

Page #	This illustrates sentences using the word “system” and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	these resources from misuse and Disruption			
22	An important component of such protective efforts is the capability to promptly identify and respond to incidents of attempted *system* intrusions.	1	• System intrusions	Network/OS
22	Agencies can better protect their information *systems* from intruders by developing formalized mechanisms that integrate incident handling functions with the rest of the organizational security Infrastructure	1	• Information systems	Enterprise System
23	Accounting for and analyzing computer security incidents are effective ways for organizations to better understand threats to their information *systems.*	1	• Information systems	Enterprise System
23	Two preventive measures for deterring *system* intrusions are to install (1) software updates to correct known vulnerabilities and	1	• Deterring system intrusions	Network/OS

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	(2) messages warning intruders that their activities are punishable by law.			
23-24	First, federal guidance, industry advisories, and best practices all stress the importance of installing updated versions of operating *system* and the software that supports *system* operations to protect against vulnerabilities that have been discovered in previously released versions.	2	• Operating system • System operations	Operating System Business Processes
24	Updating operating *systems* and other software to correct these vulnerabilities is important because once vulnerabilities are discovered, technically sophisticated hackers write scripts to exploit them and often post these scripts to the Internet for the widespread use of lesser skilled hackers.	1	• Operating System	Operating System

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
24	Since these scripts are easy to use, many security breaches happen when intruders take advantage of vulnerabilities for which patches are available but ***system*** administrators have not applied the patches.	1	• System administrators	Roles
24	Second, Public Law 99-74 requires that a warning message be displayed upon access to all federal computer ***systems*** notifying users that unauthorized use is punishable by fines and imprisonment.	1	• Federal computer systems	Operating System
24	First, many bureau ***systems*** do not have ***system*** software that has been updated to address known security exposures.	2	• Bureau systems • Do not have system software	Enterprise System Operating System
24	For example, during our review, we discovered 20 *systems* with known vulnerabilities for which patches were available but not installed.	1	• Discovered 20 systems	Operating System

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
24	Second, in performing our testing of network security, we observed that warning messages had not been installed for several network paths into Commerce *systems* that we tested.	1	• Commerce systems	Enterprise System
24	Federal guidance emphasizes the importance of using detection *systems* to protect *systems* from the threats associated with increasing network connectivity and reliance on information *systems*.	3	• Detection systems • Protect systems • Information systems	Unclear Network/OS Enterprise System
25	Although the CIO's July memo directs Commerce bureaus to monitor their information *systems* to detect unusual or suspicious activities, all the bureaus we reviewed were either not using monitoring programs or had only partially implemented their capabilities	1	• Information Systems	Enterprise System
25	For example, only two of the bureaus had installed	1	• Intrusion detection	Network Controls

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	intrusion detection *systems.*		Systems	
25	Also, *system* and network logs frequently had not been activated or were not reviewed to detect possible unauthorized activity.	1	• System and network logs	Network Controls
25	Moreover, modifications to critical operating *system* components were not logged, and security reports detailing access to sensitive data and resources were not sent to data owners for their review.	1	• Critical operating system components	Operating System
25	The fact that bureaus we reviewed detected our activities only four times during the 2 months that we performed extensive external testing of Commerce networks, which included probing over 1,000 *system* devices, indicates that, for the most part, they are unaware of intrusions.	1	• System devices	Unclear
25	For example, although we spent several weeks probing	1	• Access to many of its	Network/OS

Page #	This illustrates sentences using the word “system” and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	one bureau's networks and obtained access to many of its *systems*, our activities were never Detected.		Systems	
25	Without monitoring their information *systems*, the bureaus cannot know how, when, and who performs specific computer activities, to be aware of repeated attempts to bypass security, or to detect suspicious patterns of behavior such as two users with the same ID and password logged on simultaneously or users with *system* administrator privileges logged on at an unexpected time of the day or night.	2	• Information systems • System administrators	Network/OS Roles
25-26	For example, one bureau responded to our scanning of their ***systems*** by scanning ours in return.	1	• Responded to our scanning of their systems by scanning ours in return	Network/OS

Page #	This illustrates sentences using the word “system” and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
26	In another bureau, a Commerce employee who detected our testing responded by launching a software attack against our ***systems***.	1	• Software attack against our systems	Operating System
26	For example, the Commerce employees who responded to our testing by targeting our ***systems*** in the two instances discussed above did not report either of the two incidents to their own bureau's security officer.	1	• Targeting our systems	Operating System
27	By not reporting incidents, the bureaus lack assurance that identified security problems have been tracked and eliminated and the targeted *system* restored and validated.	1	• Targeted system restored and validated	Network/OS
27	Furthermore, information about incidents could be valuable to other bureaus and assist the department as a whole to recognize and secure *systems* against general patterns of intrusion.	1	• Secure systems against patterns of intrusion	Network/OS

Page #	This illustrates sentences using the word “system” and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
27	The underlying cause for the numerous weaknesses we identified in bureau information *system* controls is that Commerce does not have an effective department wide information security management program in place to ensure that sensitive data and critical operations receive adequate attention and that the appropriate security controls are implemented	1	• Bureau information system controls	Enterprise System
28	By providing coordination and oversight of information security activities organization wide, such a function can help ensure that weaknesses in one unit's ***systems*** do not place the entire organization's information assets at undue risk.	1	• Unit’s systems	Unclear
28	These responsibilities include developing policies, procedures, and directives for information security;	1	• Commerce systems	Enterprise System

Page #	This illustrates sentences using the word “system” and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	providing mandatory periodic training in computer security awareness and accepted practice; and identifying and developing security plans for Commerce *systems* that contain sensitive information.			
28	Commerce lacks an effective centralized function to facilitate the integrated management of the security of its information *system* infrastructure.	1	• System infrastructure	Unclear
28-29	Commerce policy also requires each of its bureaus to implement an information security program that includes a full range of security responsibilities. These include appointing a bureau wide information security officer as well as security officers for each of the bureau's *systems.*	1	• Bureau’s systems	Enterprise System
29	However, the Commerce bureaus we reviewed also lack their own centralized functions to coordinate bureau	1	• Information systems infrastructure	Enterprise System

Page #	This illustrates sentences using the word “system” and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	security programs with departmental policies and procedures and to implement effective programs for the security of the bureaus' information *systems* infrastructure.			
29	In view of the widespread interconnectivity of Commerce's *systems*, the lack of a centralized approach to the management of security is particularly risky since there is no coordinated effort to ensure that minimal security controls are implemented and effective across the department.	1	• Commerce’s systems	Networks/OS
29	As demonstrated by our testing, intruders who succeeded in gaining access to a *system* in a bureau with weak network security could then circumvent the stronger network security of other bureaus	1	• Gaining access to a system	Network/OS

Page #	This illustrates sentences using the word “system” and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
29	Federal guidance requires all federal agencies to develop comprehensive information security programs based on assessing and managing risks.28 Commerce policy regarding information security requires (1) all bureaus to establish and implement a risk management process for all IT resources and (2) ***system*** owners to conduct a periodic risk analysis for all sensitive *systems* within each bureau.	2	• System owners • Sensitive systems	Roles Enterprise System
Footnote	The February 1996 revision to OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources, requires agencies to use a risk-based approach to determine adequate security, including a consideration of the major factors in risk management: the value of the *system* or application, threats,	1	• System or application	Enterprise System

Page #	This illustrates sentences using the word “system” and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	vulnerabilities, and the effectiveness of current or proposed safeguards.			
30	Commerce bureaus we reviewed are not conducting risk assessments for their sensitive *systems* as required	1	• Sensitive systems	Enterprise System
30	Only 3 of the bureaus' 94 *systems* we reviewed29 had documented risk assessments, one of which was still in draft.	1	• Sensitive Systems	Enterprise System
30	Consequently, most of the bureaus' *systems* are being operated without consideration of the risks associated with their immediate environment.	1	• Bureaus’ systems	Enterprise System
30	Moreover, these bureaus are not considering risks outside their immediate environment that affect the security of their *systems*, such as network interconnections with other *systems*.	2	• Security of their systems • Interconnections of other systems	Enterprise System Network/OS

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
30	Appendix III specifically requires that the risks of connecting to other *systems* be considered prior to doing so, several bureau officials acknowledged that they had not considered how vulnerabilities in *systems* that interconnected with theirs could undermine the security of their own *systems.*	3	• Connecting to other systems • Vulnerabilities in systems • Security of their own systems	Network/OS Network/OS Network/OS
30	The widespread lack of risk assessments, as evidenced by the serious access control weaknesses revealed during our testing, indicates that Commerce is doing little to understand and manage risks to its *systems.*	1	• Risks to its systems	Enterprise System
30	Once risks have been assessed, OMB Circular A-130, Appendix III, requires agencies to document plans to mitigate these risks through *system* security plans.	1	• Mitigate these risks through system security plans	Enterprise System
30	These plans should contain an overview of a *system's*	2	• Overview of system's	Enterprise System

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	security requirements; describe the technical controls planned or in place for meeting those requirements; include rules that delineate the responsibilities of managers and individuals who access the *system*; and outline training needs, personnel controls, and continuity plans.		Security requirements • Individual's who access the system	Roles
30	In summary, security plans should be updated regularly to reflect significant changes to the *system* as well as the rapidly changing technical environment and document that all aspects of security for a *system* have been fully considered, including management, technical, and operational controls.	2	• Changes to the system • Security for a system	Operating System Enterprise System
30	For purposes of reviewing Commerce's information management security program, we identified these 94	1	• Sensitive Systems	Enterprise System

Page #	This illustrates sentences using the word “system” and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	sensitive *systems* in the seven bureaus based on our discussions with bureau officials.			
30	We also included *systems* from an inventory of the bureaus' most critical *systems* that had been prepared by a contractor as part of an assessment of Commerce's Critical Infrastructure Protection Plan as well as from an inventory of critical *systems* compiled by the department in preparing for their Y2K remediation efforts.	1	• Sensitive Systems • Critical systems • Critical system	Enterprise System Application Application
30	None of the bureaus we reviewed had security plans for all of their sensitive ***systems.***	1	• Sensitive systems	Enterprise System
30	Of the 94 sensitive *systems* we reviewed, 87 had no security plans.	1	• Sensitive systems	Enterprise System
30	Of the seven *systems* that did have security plans, none had been approved by management.	1	• Seven systems	Enterprise System

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
30	Without comprehensive security plans, the bureaus have no assurance that all aspects of security have been considered in determining the security requirements of the *system* and that adequate protection has been provided to meet those requirements.	1	• Security requirements of the system	Enterprise System
30	OMB also requires management officials to formally authorize the use of a ***system*** before it becomes operational, when a significant change occurs, and at least every 3 years thereafter.	1	• Authorize the use of a system	Enterprise System
30	By formally authorizing a ***system*** for operational use, a manager accepts responsibility for the risks associated with it. Since the security plan establishes the *system* protection requirements and documents the security controls in place, it should form the basis for	2	• Formally authorizing a system • System protection requirements	Enterprise System Operating System

Page #	This illustrates sentences using the word “system” and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	management's decision to authorize processing.			
30	As of March 2001, Commerce management had not authorized any of the 94 sensitive ***systems*** that we identified. According to the more comprehensive data collected by the Office of the CIO in March 2000, 92 percent of all the department's sensitive ***systems*** had not been formally authorized.	2	• Management had not authorized any of the 94 sensitive systems that we identified • 92 percent of all the department's sensitive systems had not been formally authorized	Enterprise System Enterprise System
30	The lack of authorization indicates that ***systems'*** managers had not reviewed and accepted responsibility for the adequacy of the security controls implemented on their ***systems***.	2	• Systems' managers had not reviewed and accepted responsibility • Security controls	Roles Unclear

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
			Implemented on their systems	
30	As a result, Commerce has no assurance that these ***system***s are being adequately protected. The third key element of computer security management, as identified during our study of information security management practices at leading organizations, is establishing and implementing policies.	1	• Has no assurance that these systems are being adequately protected	Enterprise System
30	Further, Commerce has no departmental policies establishing baseline security requirements for all *systems*	1	• Baseline security requirements for all systems	Network/OS
30	Consequently, security settings differ both among bureaus and from ***system*** to ***system*** within the same bureau.	1	• Security settings differ both among bureaus and from system to	Operating System

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
			System within the same bureau	
30	Furthermore, Commerce lacks consistent policies establishing a standard minimum set of access controls. Having these baseline agency wide policies could eliminate many of the vulnerabilities discovered by our testing, such as configurations that provided users with excessive access to critical ***system*** files and sensitive data and expose excessive ***system*** information, all of which facilitate intrusions.	2	• Excessive access to critical system files • Expose excessive system information,	Operating system Operating System
30	For this reason, it is vital that employees who use computer ***system***s in their day-to-day operations are aware of the importance and sensitivity of the information they handle, as well as the business and legal	1	• It is vital that employees who use computer systems in their day-to-day	Network/OS

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	reasons for maintaining its confidentiality, integrity, and availability.		Operations	
33	OMB Circular A-130, Appendix III, requires that employees be trained on how to fulfill their security responsibilities before being allowed access to sensitive ***system***s.	1	• OMB Circular A-130, Appendix III, requires that employees be trained on how to fulfill their security responsibilities before being allowed access to sensitive systems	Enterprise System
33	The Computer Security Act mandates that all federal employees and contractors who are involved with the management, use, or operation of federal computer ***system***s be provided periodic training in information	1	• All federal employees and contractors who are involved with the management, use, or	Enterprise System

Page #	This illustrates sentences using the word “system” and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	security awareness and accepted information security practice.		Operation of federal computer systems	
34	Such brief overviews do not ensure that security risks and responsibilities are understood by all managers, users, and ***system*** administrators and operators. Shortcomings in the bureaus' security awareness and training activities are illustrated by the following examples.	1	• Security risks and responsibilities are understood by all managers, users, and system administrators	Roles
34	Several of the computer security weaknesses we discuss in this testimony indicate that Commerce employees are either unaware of or insensitive to the need for important information ***system*** controls.		• Need for important information system controls	Unclear
34	The final key element of the security management cycle is an ongoing program of tests and evaluations to ensure that ***system***s are in compliance with policies and that	1	• Evaluations to ensure that systems are in compliance with	Unclear

Page #	This illustrates sentences using the word “system” and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	policies and controls are both appropriate and effective.		Policies	
34	For these reasons, OMB Circular A-130, Appendix III, directs that the security controls of major information *systems* be independently reviewed or audited at least every 3 years.	1	• Major information systems	Enterprise System
34	Commerce policy also requires information security program oversight and tasks the program manager with performing compliance reviews of the bureaus as well as verification reviews of individual ***system***s.	1	• Verification reviews of individual systems	Unclear
34	Commerce policy also requires information security program oversight and tasks the program manager with performing compliance reviews of the bureaus as well as verification reviews of individual ***system***s.	1	• Verification reviews of individual systems	Unclear
34	No oversight reviews of the Commerce bureaus' ***system***s	1	• Oversight reviews of	Enterprise System

Page #	This illustrates sentences using the word “system” and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	have been performed by the staff of Commerce's department wide information security program.		The Commerce Bureaus' systems	
34	Only one of the bureaus has performed isolated tests of its ***system***s.	1	• Performed isolated tests of its systems.	Network/OS
34	In lieu of independent reviews, in May 2000, the Office of the CIO, using a draft of the CIO Council's Security Assessment Framework, requested that all Commerce bureaus submit a self-assessment of the security of their ***system***s based on the existence of risk assessments, security plans, ***system*** authorizations, awareness and training programs, service continuity plans, and incident response capabilities.	2	• Self-assessment of the security of their systems • System authorizations	Enterprise System Enterprise System
34	This self-assessment did not require testing or evaluating whether ***system***s were in compliance with policies or the	1	• Did not require testing or evaluating whether	Enterprise System

Page #	This illustrates sentences using the word “system” and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	effectiveness of implemented controls. Nevertheless, the Office of the CIO’s analysis of the self-assessments		Systems were in compliance with policies	
34	Furthermore, the bureaus we reviewed do not monitor the effectiveness of their information security. Policies and Controls Are Not Monitored showed that 92 percent of Commerce's sensitive ***system***s did not comply with federal security requirements.	1	• Commerce's sensitive systems	Enterprise System
34	Specifically, 63 percent of Commerce's ***system***s did not have security plans that comply with federal guidelines, 73 percent had no risk assessments, 64 percent did not have recovery plans, and 92 percent had not been authorized for operational use.	1	• 63 percent of Commerce's systems did not have security plans	Enterprise System
34	These weaknesses are exacerbated by Commerce’s	3	• Vulnerabilities of	Operating System

Page #	This illustrates sentences using the word "system" and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	highly interconnected computing environment in which the vulnerabilities of individual ***system***s affect the security of ***system***s in the entire department, since a compromise in a single poorly secured ***system*** can undermine the security of the multiple ***system***s that connect to it.		Individual systems • Security of systems in the entire department • Single poorly secured system security • Of the multiple systems that connect to it	Network/OS Operating System Network/OS
36	To address these weaknesses, we are recommending that the Secretary direct the Office of the CIO and the bureaus to develop and implement an action plan for strengthening access controls for Commerce's ***system***s commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or modification of	1	• Strengthening access controls for Commerce's systems	Unclear

Page #	This illustrates sentences using the word “system” and the number of times used within a single sentence	# Used in Sentence	Context in the Sentence	Context of Word
	information resulting from unauthorized access.			
36	Specifically, this action plan should address the logical access control weaknesses and other information ***system*** weaknesses that are summarized in our draft report, direct the Office of the CIO to establish a department wide incident handling function with formal procedures for preparing for, detecting, responding to, and reporting incidents, and to direct the Office of the CIO to develop and implement an effective department wide security program.	1	• Action plan should address the logical access control weaknesses and other information system weaknesses	Enterprise System

Appendix 2

GAO Reports and Associated Findings

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
GAO-01-615 *Information Security: Weak Controls Place Interior's Financial and Other Data at Risk*	37,000 users		Access Authority: Organization must protect data supporting critical operations from unauthorized access, which could lead to improper modifications,	Center did not sufficiently restrict users	Not defined	Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Disclosure or deletion.			
GAO-01-615			Access Authority:	Users had access privileges to software libraries and sensitive systems functions, allowing security controls to be circumvented	400	.08% (assuming user base of 37,000) .37%
GAO-01-615			Access Authority:	Users were given broad access privileges to system software to modify and read programs	1,000	.04% of total users

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
GAO-01-615			Access Authority:	Users running programs, which did not require this level of access	500	
GAO-01-615			Access Authority:	Users had access, which allowed them to alter or update system resources	17	
GAO-01-615			Access Authority:	Developers had access to payroll and personnel data	80	Not defined
GAO-01-615			All Software Controls: To protect the integrity and reliability of information	Weakness in system software configuration could allow users with access privileges to bypass access controls and gain access to sensitive and financial personnel information. The Operation S	34 libraries	Not Defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Systems, it is essential to control access and modifications to the system software.	System was set up so programs in any of 34 libraries included in the normal search could perform sensitive system functions.		
GAO-01-615			All Software Controls:	Programs in sensitive software libraries would have access to perform sensitive functions	8,200	Not defined
GAO-01-615			All Software Controls:	20 of 200 software changes reviewed did not include appropriate documentation	20	10%

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
GAO-01-615			Network controls are key to ensuring authorized individuals can gain access to sensitive and critical agency data	Not adequately protecting access to the network, specifically, managing user IDS and passwords, dial-in access, or configuring network servers	Not defined	Not defined
GAO-01-615			Network Controls	Network had user ID and password management weaknesses that could allow an intruder to exploit the network	Not defined	Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
GAO-01-615			Network Controls	Server had easily guessed passwords and passwords, not used since 1998	1 server	Not defined
GAO-01-615			Network Controls	Network commands with read access to all users, including a listing that included password information	1 network	Not defined
GAO-01-615			Network Controls	User Id and password to the central modem pool were easily guessed, which allowed network browsing	Not defined	Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
GAO-01-615			Network Controls	Network had software configuration weaknesses, which allowed users to bypass controls and gain unauthorized access. Certain network settings allowed users to connect to the network	Not defined	Not defined
GAO-01-615			Program to Monitor Access Activities: Require a comprehensive program to monitor user access,	When NBC-Denver installed intrusion detection system, procedures were not developed for managing the system for 1) Determining where access is monitored; 2) protecting intrusion data; and 3) classifying, storing, and analyzing data.	NA	NA

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Including routinely reviewing user access activity to identify and investigate failed access attempts			
GAO-01-615			Other Information System Controls: Other Important Controls	People were able to access the building following a person with an access card	Several people	.008%

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Should be In Place, including Policies, Procedures, and Control Techniques Physical Controls – Important for Protecting Computer Facilities			

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Other Information System Controls:	Guards were not checking each person when they entered the building with the photo ID	Not defined	Not defined
			Other Information System Controls:	Employees had access to electrical room who should not have been authorized	40	.108%
GAO-01-615	37,000 users		Other Information System Controls:	Tape library was not controlled and room was not restricted	Not defined	Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
GAO-01-615			Computer Duties Were Not Always Segregated: Technique to protect data is to segregate responsibilities	Identified instances where controls did not enforce separation of duties. Two staff had access to financial production program s and security-related information	2	.005%
GAO-01-615			Computer Duties Were Not Always Segregated:	Not monitoring access of individuals whose roles were not separated	2	.005%

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
GAO-01-615			Computer Duties Were Not Always Segregated:	Did not provide supervisory support on weekends to computer operators	Not defined	Not defined
GAO-01-615			Changes to Application Programs: Important to ensure only authorized and fully tested program s are placed in operations	Twenty application program changes did not have changes authorized	Not defined	Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
GAO-01-615			Changes to Application Programs	Thirteen of twenty did not have specific modifications	13	Not defined
GAO-01-615			Changes to Application Programs	Procedures were not in place to test program code	NA	NA
GAO-01-615			Service Continuity Planning: Organization must take steps to ensure it is prepared to	Had not conducted unannounced tests or walk-through of disaster recovery plan. Instead, people were aware tests would take place.	Not defined	Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			cope with loss of operational capability due to earthquakes, fires, etc.			
GAO-01-615			Service Continuity Planning:	Critical backup files were not inventoried	Not defined	Not defined
GAO-01-615			Service Continuity Planning:	Plans were not tested annually	Not defined	Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
GAO-01-615			Computer Security Management: An organization needs a program to establish guidance; require performing risk assessments, raising awareness, and	Aside for computer awareness, steps were not effective. NBC-Denver did not: Establish a central security group	NA	NA

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			evaluating control effectiveness			
			Computer Security Management:	Did not do risk assessments when there was significant change	Not defined	Not defined
			Computer Security Management:	Not all policies were developed, including physical access, logical access, segregation of duties, application change control, service continuity, security management , network, mainframe, technical standards, operating system	10	Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
				Integrity for networked systems, operating system integrity for mainframes		
GAO-01-751 *Information Security: Weaknesses Place Commerce Data and Operations at Serious Risk*	7 bureaus 130 locations Note: bureau size, in 1 bureau, there are 155 Local Area	7 bureaus 1 location	Logical Access Controls: Protecting Data from Unauthorized Access System Access Controls: Required Users to Identify	Bureaus were not effectively managing user IDS & passwords to reduce unauthorized access risk, 1) to change system access & network rules 2) Potentially read, modify & delete, or redirect network traffic and 3) read, modify, & delete sensitive information. Examples:		Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
	Networks; 3,000 users; 50 states; and 80 countries w/Estimated Total Population= 24,000 Network Size = Unknown	• 120 systems • 8 firewalls • 20 routers • 15 switches • 3 additional agency servers • Number of users not	themselves and authenticate their Identity User ID and Password Controls: Used to Prevent Unauthorized Access	• Administrator accounts did not require passwords • Systems allowed users to change to blank password • Passwords easily guessed • Passwords were the same as user IDS • Vendor passwords used • Logon attempts not restricted, with one allowing the change after 273 years • Did not limit number of times a user could log onto the	None defined Not defined Not defined Not defined Not defined Not defined Not defined	Not defined Not defined Not defined Not defined Not defined Not defined Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
		defined		System • Did not protect passwords • Users stored passwords in readable files • Files with passwords were not protected • Encrypted account password could be read by 150 users	Not defined Not defined Not defined 150 users	Not defined Not defined Not defined Not defined
GAO-01-751 *Information Security: Weaknesses*			Control of System Administration Functions: Administrative	• System administration privilege, that should be granted for exceptional circumstances was granted to 20 individuals	20 users	.08%, if 24,000 users is accurate Not defined Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
Place Commerce Data and Operations at Serious Risk			Functions & Privileges Should not Exceed the Level Required to Perform their Duties	• Not all staff had been adequately trained (for how many should be administrators) • System administrators were sharing passwords on other important systems	Not defined Not defined	
GAO-01-751 *Information Security: Weaknesses*			Access to Critical Systems: Access privileges	• Not configured to restrict access to data or system files • Excessive privileges were granted to sensitive data files	Six bureaus Six bureaus	Not defined Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
Place Commerce Data and Operations at Serious Risk			should be controlled, to protect files to protect against intruders			
GAO-01-751 *Information Security: Weaknesses Place Commerce Data and Operations at*			Operating systems: Operating system controls are essential to ensure security controls function as intended. These	Systems in all bureaus were not configured to control excessive information from exposure to potential hackers & provided excessive information related to the computer	Seven bureaus	Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
Serious Risk			Must be configured to limit amount of information made available to other systems			
GAO-01-751		1 system	Operating Systems: Proper configuration of operating systems is	In a large computer system, there were thousands of important programs not assigned unique names	Thousands	Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Important for ensuring the reliable operation of computers			
GAO-01-751		1 system	Operating Systems:	Critical parts of operating system were shared in the test and production systems to process US export information	1	1
GAO-01-751		8 firewalls	Systems Configuration: Operating systems should be configured	Unnecessary and poorly configured system functions existed on important computer systems.	Defined as Limited Official Use and not Able to be	Defined as Limited Official Use and not Able to be Published

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			To support the capabilities needed by each computer system		Published	
GAO-01-751		8 firewalls	Systems Configuration:	Unnecessary and poorly configured system functions existed on important computer systems.		
GAO-01-751		8 firewalls	Systems Configuration:	Bureaus lacked effective external and internal network security controls; 4 bureaus had not configured their firewalls	4 bureaus	57%

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
GAO-01-751		8 firewalls	Systems Configuration:	Bureaus lacked effective external and internal network security controls; 6 modems were installed so that anyone could connect to the network	6	Not defined
GAO-01-751		8 firewalls	Systems Configuration:	Bureaus managed their own networks	4	57%
GAO-01-751		8 firewalls	Systems Configuration:	Interconnectivity puts all bureaus at risk	NA	NA
GAO-01-751		7 bureaus	*Other Information System*	Separation of duties were not defined	7 bureaus	100%

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Controls: In addition to access controls, other controls should be in place to ensure confidentiality, integrity, and availability. This includes policies for separation of duties, configuration			

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			management.			
GAO-01-751		7 bureaus	Software Changes: Is important to ensure only authorized and fully tested software is placed in operation.	Software change controls are not in place.	3 bureaus	42%

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
GAO-01-751		7 bureaus	Service Continuity: Organizations must ensure they are prepared to cope with loss of operational capability due to earthquakes, fires, etc.	One bureau had plans for data and software but not for the rest of its critical operations	Bureaus lacked comprehensive plans. None had completed recovery plans for all of their sensitive systems	Not defined
GAO-01-751			Service Continuity:	6 of 7 Bureaus did not have documented backup procedures	6 bureaus	85%
GAO-01-751			Service	One agreement for backup had not	1 agreement	Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Continuity:	been documented		
GAO-01-751			Service Continuity:	One bureau does not store backup files off premise	1 bureau	14%
GAO-01-751			Service Continuity:	Two facilities did not have backup facilities	2 bureaus	28%
GAO-01-751			Incident Detection: Is essential that agencies protect resources from misuse and disruption to 1) prevent 2)	Commerce incident handling is inadequate	Not defined	Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Detect 3) respond and 4) report intrusions			
GAO-01-751			Incident Handling: Need to Account for security incidents	6 of 7 bureaus have only ad hoc procedures	6 bureaus	85.7%
GAO-01-751			Incidents: Need to ensure patches are implemented and warn	Many systems do not have system software updated to protect against known vulnerabilities; were 20 systems with no patches installed	20 systems	Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Intruders that intrusions is punishable by law			
GAO-01-751			Incidents:	All bureaus running older software	7 bureaus	100%
GAO-01-751			Incident Detection: Need to establish steps to detect intrusions and take steps to correct	All bureaus had not completely installed monitoring programs	7 bureaus	100%

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
GAO-01-751			Incident Detection:	Only 2 bureaus had Intrusion Detection Systems	2 bureaus	28%
GAO-01-751			Incident Detection:	System and network logs were not activated and reviewed	Not defined	Not defined
GAO-01-751			Incident Detection:	Probing of the network was not detected	1000 devices probed	0% detected
GAO-01-751			Incident Response: Bureaus must respond to detected incidents	One bureau has documented response procedures	1 bureau	14%

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
GAO-01-751			Bureaus and Incident Reporting: Bureaus should report incidents	Bureaus have not reported all detected incidents	10+	Not defined
GAO-01-751			Effective Information Security Management Program: Must be an effective program to ensure sensitive data and critical	Commerce lacks effective centralized management. Is not specific budget to direct control and does not have sufficient resources for IT security program.		

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Operations receive adequate attention and that adequate controls are implemented. Centralized management is weak			
GAO-01-751			Risks:	Only 3 of the bureaus 94 systems	3 systems of	.03% of 93

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Understanding risk is the second key element of the information security management cycle.	Reviewed had documented risk assessments	93 evaluated	Total population not known
GAO-01-751		94	Security Plans: Security plans are required to mitigate risks	No bureau had effective security plans for all of their systems	87	7%
GAO-01-751		94	Systems Authorized:	Systems were not authorized	94	100%

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Officials must formally authorized use of the system.			
GAO-01-751	7 bureaus	7 bureaus	Need Policies: Policies must be Established and Implemented	Policies are outdated	Not defined	
GAO-01-751			Need Policies:	Technical policies are not available		
GAO-01-751			Need Policies:	Baseline security polices are not defined		
GAO-01-751	7 bureaus	7 bureaus	Security	None of the seven bureaus had	7 bureaus	100%

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Awareness: Awareness must be Promoted	Documented security training		
			Security Awareness:	One bureau did not see training as integral part of security	1	14%
			Security Awareness:	One bureau used generic training	1	14%
			Security Awareness:	Another bureau had limited awareness	1	14%
GAO-01-751	7 bureaus	7 bureaus	Policies and Controls: Agencies should monitor	No oversight reviews were conducted	7 bureaus	100%

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			To ensure there is compliance with policies and controls			
GAO-01-751			Policies and Controls:	Self assessments were not in compliance with federal requirements and did not require testing	Not defined	Not defined
GAO-01-1067*: Education Information Security: Improvements*	1,200 internal users 17,600 external users		Access Control: Protect critical data from unauthorized access, improper	Correction was not made to correct vulnerability, allowing access to the Education Central Automated Processing System (EDCAPS) web server, increasing risk for a hacker to gather	Not defined	Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
Made but Control Weaknesses Remain			Modification, disclosure, or deletion. Controls should sufficiently protect networks from unauthorized users; manage user IDS and passwords; limit access granted to authorized	Sensitive information; deface web site; or cause denial of service		

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Users; maintain system software controls; and routinely monitor access activity.			
GAO-01-1067:			Access Control:	Captured user IDS and password from an internal network connection, using readily available hacker software	Not defined	Not defined
GAO-01-1067:			Access Control:	Identified active network connections in conference rooms, which were used to gain	Not defined	Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
				Unauthorized access to system		
GAO-01-1067:	4,185	4,121	Access Control:	Passwords were easily guessed using readily available software	4,121	98%
GAO-01-1067:	4,185	4,121	Access Control:	Network IDS for all separated employees were not being deleted	175	4%
GAO-01-1067:	4,185	4,121	Access Control:	Unused IDS were not removed	860	20% 100% (Is a potential discrepancy stating about 18,800 users, when this was the total number of \users defined.

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
GAO-01-1067:	18,800 (of these 1200 are internal users and 17,600 are external users)	Not defined	Access Authority:	About 18,800 users had access privileges that allowed them to modify the database, in ways that could increase risk to integrity of EDCAPS	18,800	100%
GAO-01-1067:	18,800	Not defined	Access Authority:	Workstations were not adequately secured to prevent access to information maintained on workstations; network	Not defined	Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
				Connectivity allowed workstation access		
GAO-01-1067:	18,800 users)	Not defined	Access Authority:	Compensating controls were not established to ensure only modifications were made to the network to those users having administrative privileges, giving these people total access to the system that manages security and password database for Education's computer network	Not defined	Not defined
GAO-01-1067:			Access Authority:	System configurations were not reviewed periodically	Not defined	Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
GAO-01-1067:			Access Authority:	Servers were configured so unauthorized users could establish a network connection without entering a valid user ID and password	Not defined	Not defined
GAO-01-1067:			Access Authority:	Database was not configured to lock out access after a specific number of logon attempts	Not defined	Not defined
GAO-01-1067:			Access Authority:	Process was not established to ensure vendor enhancements to the system software were updated timely, allowing potential exposure due to common security	Not defined	Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
				Vulnerabilities		
GAO-01-1067:			Access Authority:	Had not developed procedures to control system software changes	Not defined	Not defined
GAO-01-1067:			Monitoring User Access reduces risk, created by access control problems	Education reviewed access to critical files and systems but did not have a process to routinely monitor the access of authorized users, especially those who have the ability to alter sensitive information	NA	NA
GAO-01-1067:			Monitoring User Access	Network monitoring was not used to identify patterns or established	NA	NA

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Reduces risk, created by access control problems	Intrusion detection system to log unusual activity.	NA	NA
GAO-01-1067*:*		Not defined	Other control objectives include: physically protecting resources; providing segregation of duties; preventing	Did not have approved procedures for granting access to systems.	120	Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Unauthorized application changes; and ensuring continuity of computer processing.			
GAO-01-1067:			Other control objectives	Visitor access was not recorded	Not defined	Not defined
GAO-01-1067:		4	Other control objectives	Access to wiring closets was not controlled.	3	75%
GAO-01-1067:	1200	1200	Other control objectives	Fourteen users were granted a level of access that allowed them to create recipients, approve grant	14	1.1%

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
				Amounts, change bank account data, and request payments within EDCAPS		
GAO-01-1067*:*			Other control objectives	The administrator, responsible for maintenance and day-to-day operations of the main EDCAPS computer was also responsible for moving computer programs from development to production. Dual responsibilities gave administrator the ability to alter EDCAPS data and programs, which does not comply with the basic segregation	1	Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
				Of duties principles and EDCAPS security plan.		
GAO-01-1067:	Not defined	Not defined	Application Program Controls: An application change control process shows that changes are tested, approved and implemented to prevent unauthorized	Documentation was not always maintained to show that program changes have been tested, independently reviewed, and approved for implementation.	Not defined	Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Changes for being introduced.			
GAO-01-1067:			Application Program Controls: Procedures must be in place to test program code.	Procedures were not always in place to test program code to ensure authorized changes were made.	Not defined	Not defined
GAO-01-1067:			Disaster Recovery: Without a disaster	A disaster recovery plan had not been developed for the network.		

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Recovery plan, there is a risk of losing the capability to process, retrieve, and protect EDCAPS information maintained electronically.			
GAO-01-1067:			Computer Security Management	Not all aspects of the program were not effective	Not defined	Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Program: A comprehensive security management program is essential to ensure information security controls work effectively on a continuing basis, including:			

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Security management staff; conducting periodic risk assessments; establishing appropriate policies and procedures; raising awareness; and evaluating effectiveness of			

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Established controls.			
			Computer Security Management Program:	The process for coordinating activities was not effective. For example, following a prior contractor-lead review, the action plan did not address most of the weaknesses, which also would have been program level weaknesses.	Not defined	Not defined
GAO-01-1067:			Computer Security Management Program:	A risk assessment was not performed for the network. One was performed for EDCAPS	1	50%

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
GAO-01-1067:			Computer Security Management Program:	The Education risk assessment process did not provide a framework to assess risk when major changes occurred.	NA	NA
GAO-01-1067:			Computer Security Management Program:	Security plan developed for EDCAPS and the network was not compliant with OMB Circular A-130	2	100%
GAO-01-1067:			Computer Security Management Program:	Technical standards were not developed for main computer platforms, i.e. UNIX or NT	Program Policies	Program Policies
GAO-01-1067:			Computer Security	There was not written authorization to operate for either	2	100%

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Management Program:	The network or EDCAPS		
GAO-01-1067*:*			Computer Security Management Program	Awareness requirement was not fully enforced for contractors	Not defined	Not defined
GAO-01-1067*:*			Computer Security Management Program	Was not a program to routinely ensure polices were in place to test effectiveness of awareness	Program Policies	Program Policies
GAO-04-154 *Information Security: Further*	114,000 employees 29 agencies	0 employees 2 agencies	Access to Sensitive Data: Protect Data Supporting its	Network boundaries do not provide sufficient protection and network and mainframe access controls were inadequate	Not defined	Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
Efforts Needed to Address Serious Weaknesses at USDA	7,000 offices	4 field offices 3 agency servers	Critical Operations from Unauthorized Access, which could lead to improper modifications, disclosure, or deletion Network boundaries should be secured for			

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Protecting resources from unauthorized access, manipulations, and use			
GAO-04-154			Access to Sensitive Data:	Is not established program for monitoring access	Not defined	Not defined
GAO-04-154	See Above	See Above	Network Access Controls: Requires effective network access	USDA did not always secure network services or configure devices to prevent unauthorized access	Not defined	Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Controls, such as passwords to authenticate authorized users who access the network from remote and local locations.			
			Network Access Controls:	Default vendor passwords were being used	Not defined	Not defined
			Network Access	Dial-in Modem account at 1 agency was used, for router	Not defined	Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Controls:	Management and for database management		
			Network Access Controls:	Servers configured to allow unauthorized users to connect to the network without entering valid user id and password	Not defined	Not defined
			Network Access Controls:	Password settings were inadequate	Not defined	Not defined
			Network Access Controls:	Agencies did not always comply with USDA policies	Not defined	Not defined
			Network Access	Password was not required	Not defined	Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Controls:			
			Network Access Controls:	Complex passwords were not used	Not defined	Not defined
			Network Access Controls:	Passwords were shared	Not defined	Not defined
			Network Access Controls:	Users had access, without a need to know	Not defined	Not defined
			Network Access Controls:	Potentially dangerous services were running on network systems	Not defined	Not defined
			Network	Software was not always updated	Not defined	Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Access Controls:			
			Network Access Controls:	Patches were not always updated	Not defined	Not defined
			Network Access Controls:	Servers not running antivirus software	Not defined	Not defined
GAO-04-154	17,000 users	Not defined	Effective Mainframe Access controls should be designed to prevent, limit,	• Access to data and program was not controlled. At one agency, 143 had IDS granted read access, without job responsibilities. • 11 of the 143 had access to	143 – 1 agency 11	.8% .06%

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			And detect access to computer programs and data on the mainframe. This includes assigning user rights & permissions, appropriately configuring software for granting access	Modify data • 69 users could read all data • Users had access to powerful mainframe privileges • Users could read JCL • Users could read database IDS & passwords • Password settings were not adequate • Systems not periodically reviewed	69 10 1200 800 Not defined Not defined	.4% .05% 7% 4.7% Not defined Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			And ensuring access remains appropriate			
GAO-04-154	29 agencies	2 agencies	Comprehensive Monitoring Not Yet Fully Implemented: USDA should have a fully established comprehensive program to monitor user access. This	• Logging features were not enabled for certain sensitive mainframe data files, as well as for numerous servers. • Inappropriate mainframe configuration settings allowed audit logs to be modified, potentially without detection. • USDA did not adequately review audit information or monitor system activity.	Not defined Not defined Not defined	Not defined Not defined Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Includes routinely reviewing user access activity & investigating failed attempts to access critical programs & data.	Where audit logs existed, these were not always reviewed for certain servers. • One agency had not implemented Intrusion Detection System	1 agency	50 % of those reviewed or .03% of total number of agencies
GAO-04-154	114,000 employees		Other Information System Controls: Other	Agencies did not always ensure access to resources were granted to those who needed access to perform jobs	Not defined	Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Important controls should be in place: Physical Security controls are required to protect facilities.			
GAO-04-154			Other Information System Controls:	One agency had not developed an access control policy for sensitive areas	1 agency	50% of sample or .03% of total
GAO-04-154			Other	Cards for contractors remained	Not defined	Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Information System Controls:	Active, when no longer needed		
GAO-04-154			Other Information System Controls:	Two cards were lost	2	Not defined
GAO-04-154			Other Information System Controls:	Computer resources were not always secured; one door did not have a lock	1 door	Not defined
GAO-04-154			Other Information System	At one agency, server rooms in two of the four field offices were unlocked.	Two offices	50% of the offices Reviewed

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Controls:			
GAO-04-154		Not defined	System Software Controls: Software controls which limit and monitor access to powerful programs are important in providing that access controls are not	A sensitive program was configured, so that it could affect system integrity.	1	Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Compromised.			
GAO-04-154		Not defined	System Software Controls:	Software libraries, which have authority to perform sensitive functions that can circumvent program s, have duplicate names.	Not defined	Not defined
GAO-04-154		Not defined	System Software Controls:	Programs were not checked for duplicate names	Not defined	Not defined
GAO-04-154		Not defined	System Software Controls:	Software approvals, testing, and implementation documentation were not always maintained.	Not defined	Not defined
GAO-04-154	29 agencies	2 agencies	Application Change	One agency did not develop policies to ensure software	1	50% of sample or .03% of total

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Controls: Need to ensure only authorized and fully tested software is placed in operation	Modifications were authorized		number of agencies
GAO-04-154	29 agencies	2 agencies	Application Change Controls:	Several agencies did not adequately protect software libraries (Only two agencies were defined as reviewed so this causes some confusion)	Several agencies	Not defined
GAO-04-154			Service	Agencies had not developed	1	60% had a plan

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Continuity Planning: Must ensure that agency is adequately prepared to cope with the loss of operational capability due to earthquake, fire, etc.	Contingency plans for all operations.		
GAO-04-154				Agencies had not tested contingency plans for all		30% had not tested plans

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
				Operations.		
GAO-04-154				One agency had not developed service continuity plans		
GAO-04-154				One agency was outdated	1	
GAO-04-154				Third agency had not developed service continuity plan for the network	1	
GAO-04-154				Service continuity plans had not been tested		
GAO-04-154				Eight of ten agencies had not prepared disaster recover plans. (This is not clear. 2 agencies were defined as being evaluated; report	8	

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
				States 8 of 10 had not developed plans; This could be a miscount on the 04 report or an old report finding).		
GAO-04-154			Initiatives: Need to improve security and develop a comprehensive management program to ensure controls are established.	There is a lack of management involvement in the security program.	Not defined	Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
GAO-04-154 *Information Security: Further Efforts Needed to Address Serious Weaknesses at USDA*		1	Designating a senior agency information security officer	Key elements are not implemented. Agency security officer does not have authority to implement and manage the program.	1	100% of USDA
GAO-04-154			Assessing risk: conducting a periodic assessment of risk.	Agency risk assessments have not been completed.	46	78% Complete Validated at 0%

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
GAO-04-154				Validation of risk assessments showed one agency failed to complete 46 risk assessments	46	Not defined
GAO-04-154	29 agencies	2 agencies	Establishing policies: Need to establish and implement policies & procedures, based on cost effective & Risk-based approaches.	Policies have been developed but are still in draft	2	100
GAO-04-154	29 agencies	2 agencies	Establishing	None of the agencies reviewed	2	100

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Policies:	Had developed all security plans, as required		
GAO-04-154	114,000		Security Awareness: Need to promote awareness and training.	Agencies do not provide adequate awareness training		59% of employees had not received training
GAO-04-154	7,000 offices	Not defined	Testing and Evaluation of Controls: Ongoing testing and evaluation must take place	Compliance was reviewed at 5 sites in 2003	5 sites	.0007%

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			To ensure compliance with policies.			
GAO-04-154	7,000 offices	Not defined	Testing and Evaluation of Controls:	Conducted testing of USDA network	Not defined	Not defined
GAO-04-154	7,000 offices	Not defined	Testing and Evaluation of Controls:	Was limited ongoing testing	Not defined	Not defined
GAO-03-564T *Information Security: Progress Made, But*				Network not configured in accordance with security policies		

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures						
GAO-03-564T				Default vendor accounts being used	Not defined	Not Defined
GAO-03-564T				Servers configured to allow unauthorized users to access network	Not defined	Not Defined
GAO-03-564T				Password settings are incorrect	Not defined	Not Defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
GAO-03-564T				Accounts are not created on need-to-know basis	Not defined	Not Defined
GAO-03-564T				Dangerous services are running	Not defined	Not Defined
GAO-03-564T				Agencies do not always update software	Not defined	Not Defined
GAO-03-564T				Access to sensitive systems & data not controlled	Not defined	Not Defined
GAO-03-564T				143 users granted read access to mainframe sensitive files	143	Not Defined
GAO-03-564T				Users had unnecessary privileges	Not defined	Not Defined
GAO-03-564T				All users could view a very	Not defined	Not Defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
				Powerful ID and password		
GAO-03-564T				1200 users could read JCL	1200	Not Defined
GAO-03-564T				Password MF settings were not correct	Not defined	Not Defined
GAO-03-564T				User actions not monitored	Not defined	Not Defined
GAO-03-564T				Auditing not enabled on MF	Not defined	Not Defined
GAO-03-564T				Agencies did not review MF audit information	Not defined	Not Defined
GAO-03-564T				IDS implemented but not at all sites	Not defined	Not Defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
GAO-03-564T				Are insufficient physical security controls	Not defined	Not Defined
GAO-03-564T				Inadequate background investigations	Not defined	Not Defined
GAO-03-564T				Inadequate application controls for changes	Not defined	Not Defined
GAO-03-564T				Incomplete continuity planning	Not defined	Not Defined
GAO-04-630 *Information Security: Information*	6,300 users	Not defined	Access Authority: Protect data supporting	Access to data was not sufficiently restricted. Many users had access to production systems that includes financial and bank	Not defined	Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
System Controls at the Federal Deposit Insurance Corporation Note (LOU report may contain exact numbers and percentages)		Not defined Not defined Not defined	Critical operations from unauthorized access, which could lead to improper modification, disclosure or deletion.	Information. Were granted access that could allow users to gain access to critical financial management information.		
GAO-04-630			Access Authority	An undetermined number of users were systems developers.	Not defined	Not defined
GAO-04-630			Access	Large number of users had access	Not defined	Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Authority	that allowed them to read powerful user identification and password used to transfer data among production systems.		
GAO-04-630			Access Authority	Did not restrict users from viewing sensitive information. Users had unrestricted access to read bank information.	Not defined	Not defined
GAO-04-630			Access Authority	Has not fully implemented procedures for access control.	Not defined	Not defined
GAO-04-630	6,300 users	Not defined Not defined Not defined	Network Security: It is essential to effectively	Network was not configured to restrict access to sensitive information.	Not defined	Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
		Not defined	Secure networks for protecting computing resources and data from unauthorized access, manipulation, and use. This can be done with 1) firewalls 2) routers 3)			

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Switches and 4) servers.			
GAO-04-630			Network Security:	Access connectivity was not adequately restricted	Not defined	Not defined
GAO-04-630			Network Security:	Certain network connections to off-site locations were not adequately controlled	Not defined	Not defined
GAO-04-630			Network Security:	Did not secure the network against known software vulnerabilities.	Not defined	Not defined
GAO-04-630			Fully Monitor Access: Require a	Policies were not fully implemented.	Not defined	Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Program to fully monitor user activities. This includes monitoring logs of mainframes, network servers, and routers, and Intrusion Detection Systems (IDS).			
GAO-04-630			Fully Monitor Access	Network IDS did not monitor all network traffic originating from	Not defined	Not defined

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
				Certain locations		
GAO-04-630			Fully Monitor Access	Certain network services were not configured to monitor network traffic	Not defined	Not defined
GAO-04-630			Fully Monitor Access	Duties were not segregated	Not defined	Not defined
GAO-04-630	6,300 users NA	NA NA	Implementing a computer security program effective controls must be maintained,	Completed all of the items but failed to test and evaluate the environment	NA	NA

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Including central management; risk-based policies & procedures, awareness training, assessments of risk, and periodic testing.			
GAO-04-630			Implementing a Computer	Test process does not address: Key resources; information	NA	NA

Document # & Title	Population Size	Sample Size	GAO Criteria	GAO Finding	# Occurrences	# or % of Total Population
			Security Program	Security weaknesses; independent testing; and newly identified weaknesses.		

Appendix 3

Presentation of Concept Paper for GAO Feedback

On November 29, 2004, from 10AM – 12:00 noon, a presentation was provided GAO on the concept paper, related to *Maximizing Value of IT Security Audits*. The primary goal of the presentation was to present this to GAO, as a stakeholder, in the need for government agencies to be able to receive more value from the IT security audits.

Relating to the concept, GAO provided the following feedback. First, in the concept paper, an example of fraud was used. For this example, GAO indicated this was a poor example, as there were other problems with the fraud study, in addition to IT security. Second, the concept paper provided a reference to the National Academy of Science (NAS, 1991) stating lack of training was a potential cause of poor IT security. GAO disagreed, stating this was primarily a management issue. Third, GAO personnel indicated that there was no need to use research methods to conduct an IT security review. Research methods such as using concepts of validity and reliability, and using measured samples to measure the IT environment did not apply to this organization. While this is good in an academic organization, GAO did not feel there was any use for the research concepts in looking at IT security problems. Fourth, when GAO provides reports, these are written in a very technical level. Even though these cannot be understood without the limited official version of the report, GAO personnel stated that these reports accurately reflect the IT environment and that federal agencies have concurred on the results of these reports. Fifth, GAO intentionally does not prioritize findings. This is the federal agency's responsibility to prioritize findings. In addition, there is no need to prioritize the most serious system flaws for an agency. GAO is only providing an assessment at one point in time. GAO assessments are based upon critical points in an organization. The objective of the audit is not to

present all findings but to focus on an area, which as been raised to them for attention. Sixth, GAO indicated there is no real value to prioritizing findings. For example, in the concept paper, one GAO report was used as an example, where the concept paper indicated a finding of less than 1% was statistically insignificant. GAO disagreed stating that a finding related to root access, is significant, even if occurring less than 1% of the time. Because a critical finding occurred at all, GAO viewed this as severe, since root access potentially allows anyone to access the system. In addition, GAO has an expectation of 100% compliance of all findings, since all areas being evaluated are critical. Seventh, GAO personnel do not view the GAO public versions of the reports as a management tool for other agencies to learn from but only to provide a public version of an assessment for which GAO conducted the assessment. The comments from GAO have been incorporated into the final dissertation, as appropriate.

Appendix 4: Introduction of the Delphi Process as Part of the Audit Process

4.1. Ten Step Security Delphi Model

This section introduces the Ten Step Security Delphi Model as a tool for increasing the value of IT Security audits, allowing organizations to prioritize security weaknesses, and use risk-based approaches to identify and correct the most important security flaws first. The primary goal of using a Delphi-based approach is to allow for open communication among stakeholders to discuss issues, as necessary. Better communication and information flow is critical to allowing better decision-making.

4.2. Provides Prioritization, When We Cannot Fix All Problems

As federal agencies secure IT systems, there may be a thousand or more interrelated controls and configurations, required for an operating system. For example, if an evaluation is conducted of the operating system and the system is 75% secure, there are still going to be 250 individual configurations which must be corrected. As an IT development and/or security organization, the following questions must still be answered:

1) Why were the 250 configurations not applied?
2) Did the 250 configurations cause another part of the system to fail?
3) If a part of the system failed, which configurations could be applied and still allow an application and/or system to process?
4) How many of the 250 configurations expose the network to serious vulnerabilities?
5) Can these all be corrected at once?
6) Will these be reconfigured by an application or operating system problem, once these are corrected?

7) Was there a conscious decision to retain some of the incorrect configurations or was this a mistake?

8) Are there certain controls, which should be corrected immediately?

It is quickly apparent that even with 250 wrong configurations, these may not all be corrected immediately. Research will be required to determine the cause of the problem; define alternate solutions; and identifying a best solution; and an approach to monitor configurations in the future for compliance.

More importantly, a priority must be established, to determine which findings and/or weaknesses are the most important. Agency personnel must establish and define priorities to allow funding and resources to be committed to correct key security areas.

The Delphi method can be used to improve the audit process. The Delphi method is an accepted forecasting tool, which has been used in business for several decades. More importantly, the Delphi process is a communication tool, providing a structured approach to bring people and ideas together to solve complex problems, (Turoff & Hiltz, 2004).

The Delphi method is an established communication tool, allowing a panel of selected experts to work together to obtain consensus on key problems and issues and to develop a roadmap or timetable for future developments (Encyclopedia4u, 2004). The method allows for a repetitive process to be used to develop answers and to reach consensus on unusual problems. The process used to rank and prioritize issues is an accepted management, academic, and business practice, which has been established and used for almost thirty years. By adopting this methodology, audit issues can be discussed and better understood to allow prioritization and resolution of audit issues.

This method provides a communication structure is used to facilitate communication on a specific task and usually involves anonymity of responses, feedback to the group as a whole of individual and/or collective views and the opportunity for any respondent to modify an earlier judgment, (Delphi, 2004). The Delphi method was developed at the RAND Corporation by Olaf Helmer and Norman Dalkey (Turoff, 2004, p. 3).

4.3. How Does the Delphi-Process Work

The Delphi technique allows a large group to arrive at decisions to complex problems by improving the communication techniques to allow all opinions to be heard and discussed and to allow a consensus building approach to be used to discuss and resolve the complex issues.

Since the development of the process, the Delphi method has been expanded to be used in the business world for solving complex problems, including futures building and scenario building for large organizations. For example, the technique was used by France as a way to strengthen relationships in the agrifood sector, with the change in legislation and the effects of Mad Cow disease, (Lafourcade & Chapuy, 2000). Using the Delphi process for scenario-building, this process allowed smaller and medium-sized businesses to work together to reflect on the future and to provide input into a situation, which would directly impact their own future. In this particular process, the outcome was that of a working relationship to make better decisions.

The approach used for the Delphi process, for the agricultural problem, included the following: 1) the entire group, using 40 participants, was provided with a 2-day seminar for training and exercises to understand the process and to learn how this process could help build their own future. Next, the process was documented to allow the group to be able to repeat the process with their own group. The group was also asked to write up priority concerns. There

were three rounds of surveys used, using a color-coded voting system. Over the course of a year, six additional meetings were held to use these techniques to build scenarios, investigate possible futures, and develop strategies.

Turoff and Hiltz identify key components used in the Delphi process. These key components to using the Delphi process include: anonymity of individuals contributing ideas; sessions, which are moderated and facilitated by a smaller group and/or committee, structure, allowing contributions to be made using a group view; building trend models to show relations and trends provided by the group; discussion of key issues; analysis of issues, modeling, and strategic planning.

The example uses futures building and demonstrates the flexibility of the process to resolve unusual and complex problems. The Delphi method was originated for the field of information technology and can easily be applied to IT security concepts.

4.4. Why Use Delphi Method instead of a Risk Assessment?

Today, risk assessments allow risk and cost to be balanced and measured. The Delphi Method allows for other organizations to be involved in the decision-making process, including business stakeholders. This is an important concept, especially when federal agencies are competing for financial resources and business requirements must be included into the equation of resource allocation.

In using a risk assessment methodology, the needs of the business are not always addressed. For this reason, it is significant to look at processes, which integrate a holistic business approach.

4.5. Benefits of Ten Step Security Delphi Model for Studying IT Security Issues

There are many benefits to using the Ten Step Security Delphi Model to discuss IT security problems. All of these will lend to obtaining better information and the ability to make better management decisions in the area of IT security.

Too often, especially at the national level, federal agencies rely on one or two key personnel within an agency to address security issues, including developing requirements, evaluating effectiveness of program performance, and establishing priorities for correction of IT security problems. In addition, these problems are usually addressed internal to the IT security organization.

The problem with this approach is that the agencies are then held accountable for meeting the priorities of the IT security organization. These priorities may have been made without understanding competing requirements of other organizations within the agency, such as legal, operational, etc. By using a Delphi-related process, IT security problems can be expanded to include not only other competing organizations but also to include a larger group of IT security personnel, moving from a single national group to a collaborative group of IT personnel, throughout the agency.

By bringing together groups of subject matter experts and interested stakeholders, the government agencies will be able to have more input, more feedback, and ultimately a more sound security program.

As problems arise, not all problems are of interest to all parties. By using a Delphi-related process, individuals may participate in areas which are of concern to their own organization and to their own technical specialties and interests.

The Ten Step Security Delphi Model promotes a controlled communication structure, using a small group facilitator. By providing a structure to communication, the agency will ensure that all voices are heard and that individual responses are compiled into group responses. In addition, by using a structured approach, all personnel participating in the Delphi method will understand the goals and advantages of building a joint IT security future and as a result will provide more value-added participation.

With many stakeholders, analysis of information is a key benefit to using the Ten Step Security Delphi Model. IT security personnel may have insight into technical problems but may not understand new technological solutions. By providing an analysis of the information, questions, which may arise during the ranking process, can be asked or responses clarified.

Formal methods will allow sound processes be used to weight and scale security priorities. Profiles can be created so that the profile allows a manager to view all security measures in place, at a glance, using graphic representations. By using valid management tools, the entire process provides more credibility to the organization. Sound management decisions are more readily accepted within an agency and accepted decisions are usually the easiest ones to implement.

Since all personnel have different experiences and different organizational requirements, it is important to build in opportunities for disagreement. This not only creates a learning opportunity but also provides the necessary information to show how consensus was obtained. The Delphi process allows for this disagreement, as part of the process.

Too often, when Total Quality Management (TQM) approaches are used, such as brainstorming, the ideas of others are not accepted. However well intended this approach is, there are problems whenever we bring people together: 1) there are silent members of the group,

where they have valuable input but refuse to speak; 2) one or two members will dominate the sessions; 3) the sessions are not facilitated and result in chaos.

By using a formal methodology to provide and review responses, using anonymous input, the atmosphere is more favorable and it is often easier to reach a group consensus from all stakeholders.

The final benefit of using the Delphi process will be an accepted consensus-based list of security priorities, using a consensus-based approach. This approach can be used to prioritize problems, research solutions, and eventually build a fully integrated and effective IT security program. In addition, the program will have been ranked, prioritized, and selected, using a formal verification and decision-making process.

4.6. Methodology: Ten Step Security Delphi Model

Federal agencies already prioritize security issues. The situation is that these processes do not account for the business needs, as security concerns are being prioritized.

Computer Security Incident Response groups (CSIRC) and other response organizations meet to identify corrective actions, when a system is intruded upon. Hot fixes are provided to federal agencies and gap areas are closed to intruders, as these are discovered. In these situations, these often present all high priority items.

Managers must have a mechanism to prioritize, taking all stakeholders into account, as security is built into the environment. There are ten steps required to use the Delphi process in analyzing IT security issues. A timeframe has not been identified for each of these steps. This time may vary, due to the complexity of the issues, establishment of groups, etc.

Step 1: Establish a group and conduct training

First, establish a group to address the security issues. Typically, the initial group should be large enough to include all stakeholders but small enough to enable consensus-based decisions. In addition, the team should be selected from a level of the organization, where team members will have the ability to make decisions for the organization. The recommended size should be no more that 20 people.

The group should be brought together to allow training to be given to the group. The training will allow the team to understand the process, what is trying to be accomplished and to provide the team members with expectations for each of the team members. The training will include the use of the Delphi process and the use of this process to build organizational scenarios.

Step 2: Develop Questionnaire

A questionnaire must be developed and worded to allow categories to be identified, using real organizational problems. This questionnaire should be tested for wording with the group and all members should ensure the questionnaire can easily be understood by everyone.

Step 3: Round 1 to Identify Serious Problems

The questionnaire will be sent out and members will be are asked to identify the most serious problems within the agency. In the case of maximizing value of IT security audits, the audit findings should be grouped into specific categories to allow categories to be identified.

Step 4: Collect and Compile Results

The results will be collected anonymously, by a facilitator, and compiled into a report and distributed to the team. Once the results are collected, the group will be brought together to be briefed on the categories.

Step 5: Round 2 to Identify Serious Problems

The questionnaire will be sent out again, for a second iteration. Most likely, there will be multiple categories which have equal weight. The objective is to receive consensus on several key priorities, which may require multiple rounds.

Step 6: Discuss Concerns

The group should meet and discuss why each of these concerns is relevant and/or important for these groups. This should always occur after the compilation of information to allow discussion to take place.

Step 7: Iterative Round

This step is a repeatable step to ensure the top priorities can be identified, using a consensus based approach.

Step 8: Analyze Responses

The group will focus on key issues and will develop the scenario on how to correct and implement corrective actions.

Step 9: Prepare Report

A report should be prepared to document the process, stakeholders, and decisions made relative to the issues and the scenario built to address problems.

Step 10: Measure Feedback and Provide Continuous Monitoring

At Step 10, the high priority issues will have been initiated. At this pint, the group will work together to determine if the steps have worked, if key issues were properly defined, and provide feedback on next steps with remaining issues and scenario building.

Ultimately, the organization should be able identify and work on key security issues. As with any effective program, the monitoring of the program must continue to allow the

organization to always work on organizational priorities, based upon risk and other competing factors for the organization.

Related to obtaining feedback, there are generally ten steps identified in the method, including: 1) Form a team for a given subject; 2) Select one or more panels; 3) Develop a first-round questionnaire; 4) Test the questionnaire for wording; 5) Transmit the first round; 6) Analyze responses; 7) Prepare second round; 8) Transmit second round of questionnaires; 9) Analyze second round of responses; 10) Prepare a report.

Key concepts in the Delphi process are anonymity, feedback, allowing the use of expert opinions to be used to reach consensus on key problems. Using this concept, the Delphi Mode can be applied to security-related issues, allowing all stakeholders to become involved in building a security environment, using sound management principles.

The Ten Step Security Delphi Model allows the complex issue of IT security to be discussed among the different stakeholders. This allows for all stakeholders to express concerns in an equal manner, rather than having power struggles among the various stakeholders. This is very important for any agency dealing with security issues.

By providing this communication, this allows risk-based approaches to be used in decision making and allows the risk-based approach to be assessed both individually and collectively by IT security experts, business owners, and all impacted individuals of IT security.

One of the challenges in today's IT security environment is that there are many topics, which impact IT security, where topics are all complex and often subjective. Almost always, the IT security requirements must compete against opposing goals, such as new technology.

For example, while the National Academy of Science earlier discussed the need to provide advanced training as a key initiative, the President's Commission on Critical

Infrastructure cites the need for research to Identify and understand networked vulnerabilities; avoiding implementation errors; new approaches for communication security; and building trustworthy systems from un trusted components, (National Research Council, 1999, pp. 1-11). Tipton & Krause cite the need to provide access controls over critical resources and discuss access control methodologies, related to computer systems, (Tipton & Krause, 2001).

Depending upon the context of the problem, the focus of the IT security issue will bear different weights for different people. While these topics are all important, with the limited resources, federal agencies must be able to allocate time and money to the most important decisions, using risk-based and sound management-based approaches.

Within an agency, different business organizations may have different objectives and goals than IT security. While security must be integrated into the environment, the overall function and goals of the organization cannot be ignored. Just as the National Research Council promoted the need for research related to critical assets, the National Research Council also stated that the delivery of the new digital government services was dependent on access to information technology, (National Research Council, 2002, p.7). The council recommended that the government should adopt commercial technologies and associated practices wherever possible. Unfortunately, new technologies are the areas where the security vulnerabilities always appear first. By having the conflicting goals, personnel within agencies must work together to ensure all goals for the agency are prioritized and addressed, using an integrated approach.

4.7. Summary of Ten Step Security Delphi Model

The Ten Step Security Delphi Model provides a forum to establish agreed-upon security priorities, for federal agencies. By employing processes of structured communication and consensus building, federal agencies may be able to make better decisions within the field of IT

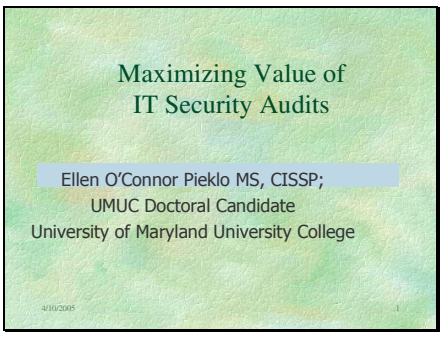
security. The primary advantage with this model is that all stakeholders have the opportunity to weigh in on IT security decisions.

Appendix 5

GAO Presentation

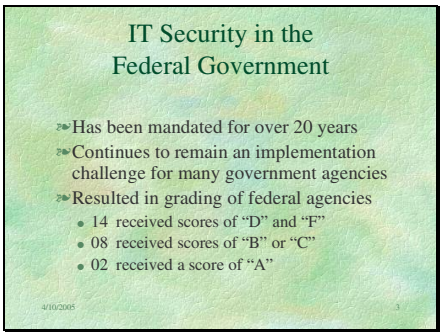
The GAO presentation, *Maximizing Value of IT Security Audits*, was presented on Monday, November 29, 2004 at GAO in Washington, DC. The presentation contains the PowerPoint slides, provided to GAO as part of this briefing.

Slide 1

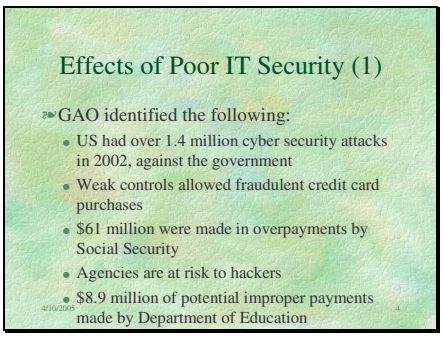


Slide 2

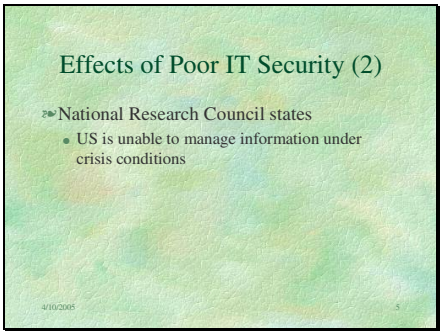
Slide 3



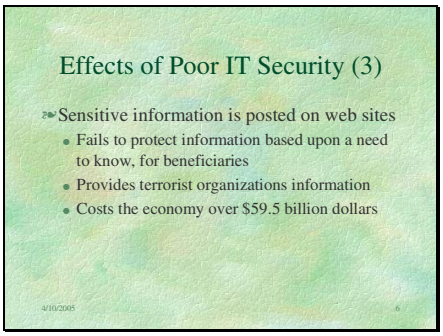
Slide 4



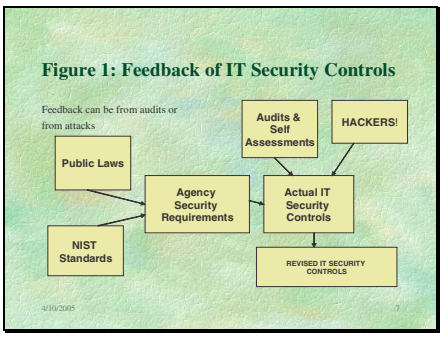
Slide 5



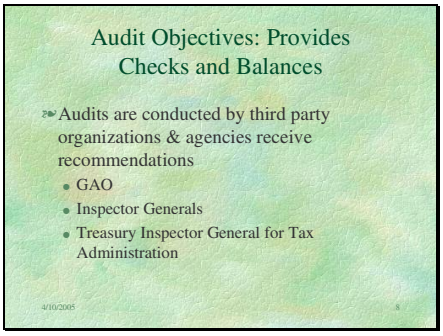
Slide 6



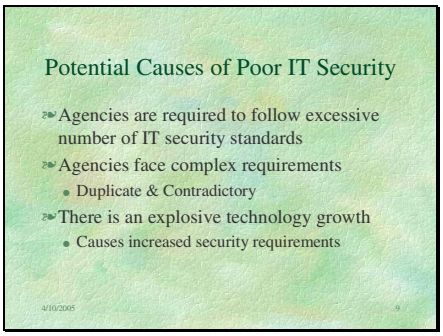
Slide 7



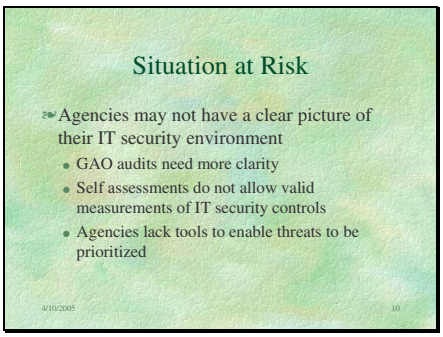
Slide 8



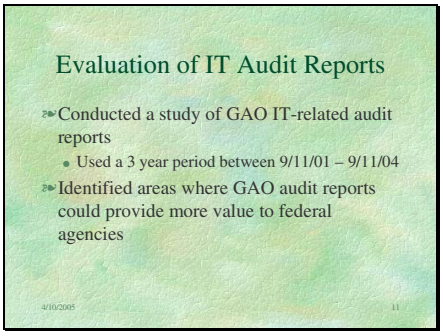
Slide 9



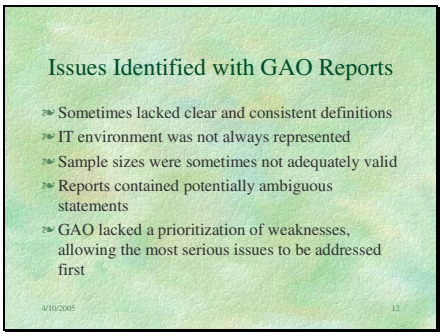
Slide 10



Slide 11



Slide 12



Slide 13

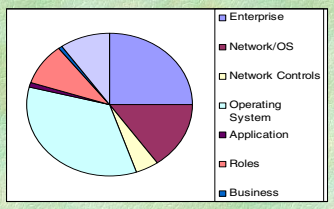
Sometimes Lack Clear Definitions

- Evaluated GAO-01-1004T Information Security: Weaknesses Place Commerce Data and Operations at Serious Risk
  - Report contains 36 pages
  - 317 uses of the word "System"
  - Used in 8 different contexts

4/10/2005 13

Slide 14

Multiple Uses of "System"



4/10/2005 14

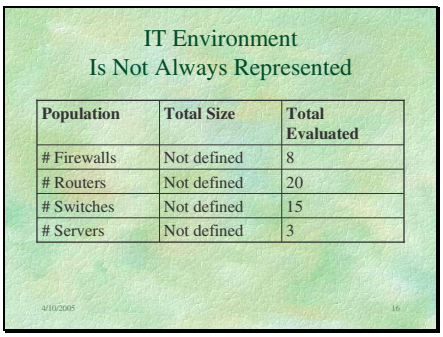
Slide 15

IT Environment Is Not Always Represented

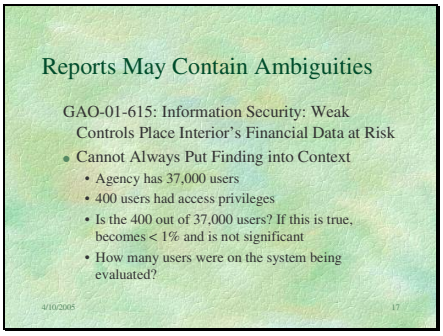
Population	Total Size	Total Evaluated
# Locations	130	1
# Countries	80	1
Local Area Networks	155	Not defined
# Users	3,000	Not defined
# Systems	94	120

4/10/2005 15

Slide 16

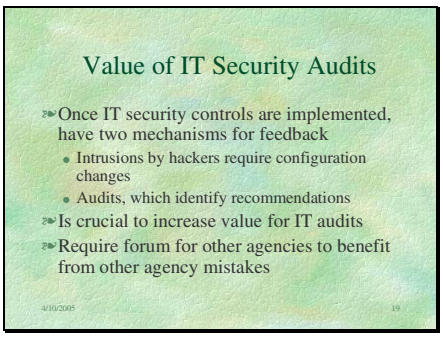


Slide 17

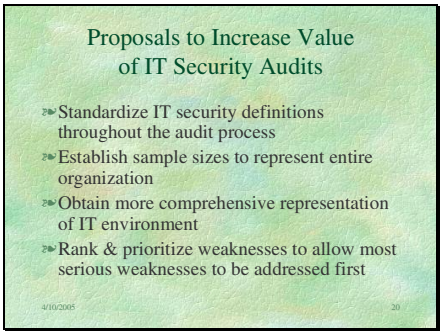


Slide 18

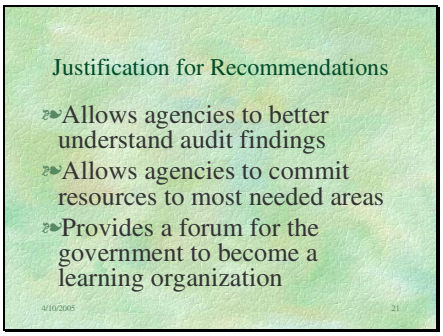
Slide 19



Slide 20



Slide 21



Slide 22