



Student Financial Assistance

Risk Assessment Guide

Prepared by:



February 7, 2002

TABLE OF CONTENTS

- 1.0 INTRODUCTION..... 3**
 - 1.1 Background..... 3
 - 1.2 Purpose..... 3
 - 1.3 Scope..... 3
 - 1.4 Report Organization..... 4

- 2.0 RISK ASSESSMENT APPROACH..... 4**
 - 2.1 Step 1 – Define System Boundary 5
 - 2.2 Step 2 – Gather Information 5
 - 2.2.1 Interviews..... 5
 - 2.2.2 Site Visit..... 6
 - 2.2.3 Documentation..... 6
 - 2.2.4 Network Scanning..... 6
 - 2.3 Step 3 – Conduct Risk Assessment..... 6
 - 2.3.1 Documenting Vulnerabilities 7
 - 2.3.2 Impact 8
 - 2.3.3 Likelihood 9
 - 2.3.4 Risk..... 11

- 3.0 SYSTEM CHARACTERIZATION 12**
 - 3.1 System Overview 12
 - 3.2 System Interfaces 12
 - 3.3 Data..... 13
 - 3.4 System and Data Criticality and Sensitivity 13
 - 3.4.1 Criticality..... 13
 - 3.4.2 Sensitivity..... 13
 - 3.4.2.1 Confidentiality: 13
 - 3.4.2.2 Integrity:..... 13
 - 3.4.2.3 Availability: 14
 - 3.5 Users 14

- 4.0 THREAT STATEMENT 16**
 - 4.1 Threat Sources 16
 - 4.2 Threat Actions..... 17

- 5.0 FINDINGS..... 17**

EXECUTIVE SUMMARY

The mission of the Department of Education's (ED) INSERT SYSTEM NAME is TO INSERT DESCRIPTION FROM INVENTORY REVIEW.

IF YOU USED CONTRACTOR SUPPORT, INSERT DESCRIPTION OF CONTRACTOR USED TO PERFORM THE WORK, INCLUDING CONTRACT #, CONTRACTOR NAME, AND PERIOD OF PERFORMANCE.

To identify the potential threats and vulnerabilities associated with the INSERT SYSTEM NAME, INSERT RISK ASSESSMENT CONTRACTOR gathered information through the following techniques:

LIST ANY THAT APPLY

- Document review,
- Site visits to the INSERT SYSTEM NAME computer room,
- Interviews with designated SFA management and technical personnel, and
- Network scanning using an automated tool.

This report documents risk assessment activities in the following security domain areas:

- Management Security,
- Operational Security,
- Technical Security, and
- Administrative Security.

A total of INSERT NUMBER OF OBSERVATION/RISKS observations were made in the areas of management, operational, and technical security. Table ES-1 presents these observations, providing observation numbers and descriptions, as well as associated risk levels. The risk associated with each observation is described as high, medium, or low, as defined below. The risk level represents the degree or level of risk to which SFA assets and resources may be exposed.

High Risk. A threat is at least moderately likely to exploit the identified vulnerability, and such exploitation is likely to severely and adversely affect INSERT SYSTEM NAME tangible and intangible resources. This level of risk indicates a strong need for corrective measures and actions, and a plan must be developed to incorporate these actions within a reasonable period of time.

Medium Risk. The exploitation of the identified vulnerability by a threat is possible, and such exploitation is likely to affect INSERT SYSTEM NAME significantly, indicating the loss of some tangible assets or resources, which could impede the INSERT SYSTEM NAME's mission, reputation, or interest. This level of risk indicates corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.

Low Risk. The identified weaknesses may be subject to exploitation by a threat, but the probability of exploitation is low, and the impact on SFA would be minor. This level of risk

indicates that SFA management should be cautioned and corrective measures applied where required.

Appendix A details the observations, presenting the observation number and description, vulnerabilities and threats, potential impacts, likelihood, priority, and recommendations for each observation.

OBSERVATION NUMBER	VULNERABILITY DESCRIPTION	RISK LEVEL
Management Security		
INSERT OBSERVATION NUMBER (M1, M2, ETC)	INSERT OBSERVATION/VULNERABILITY STATEMENT	INSERT RISK LEVEL (HIGH, MEDIUM, LOW)
Operational Security		
INSERT OBSERVATION NUMBER (O1)	INSERT OBSERVATION/VULNERABILITY STATEMENT	INSERT RISK LEVEL (HIGH, MEDIUM, LOW)
Technical Security		
INSERT OBSERVATION NUMBER (T1)	INSERT OBSERVATION/VULNERABILITY STATEMENT	INSERT RISK LEVEL (HIGH, MEDIUM, LOW)
Administrative Security		
INSERT OBSERVATION NUMBER (A1)	INSERT OBSERVATION/VULNERABILITY STATEMENT	INSERT RISK LEVEL (HIGH, MEDIUM, LOW)

Table ES-1

1.0 INTRODUCTION

1.1 BACKGROUND

INSERT SYSTEM DESCRIPTION FROM EXECUTIVE SUMMARY

1.2 PURPOSE

The purpose of this report is to provide the Department and SFA management with an assessment of the adequacy of the management, technical, operational and administrative security controls used to protect the confidentiality, integrity, and availability of INSERT SYSTEM NAME. This risk assessment report identifies threats and vulnerabilities applicable to INSERT SYSTEM NAME; the impact associated with these threats and vulnerabilities; the likelihood that a vulnerability will be exploited; countermeasures in place to mitigate the risk; and the existence of any residual risk.

This report documents the risk assessment activities that INSERT CONTRACTOR NAME performed from INSERT MONTH AND DAY, 2002 to INSERT MONTH AND DAY, 2002, and will help SFA management understand the security posture of INSERT SYSTEM NAME and its risk exposure. The risk assessment is part of SFA's continuing effort to ensure compliance with Federal policies, laws and guidance as well as the Department's IT Security Policy.

1.3 SCOPE

This risk assessment is limited to the INSERT SYSTEM NAME. INSERT DESCRIPTION OF RISK ASSESSMENT SCOPE. FOR EXAMPLE, "WHICH IS A MICROSOFT ACCESS '97 DATABASE, ITS HOST GENERAL SUPPORT SYSTEM (GSS) EDNET SERVER ROB3FPR02\GROUPS\OEP, AND THE REMOTE ACCESS SERVER (RAS). THE SERVERS ARE HOUSED IN ROOM 1234 AT THE DEPARTMENT'S ROB3 FACILITY. SFA STAFF ACCESS *INSERT SYSTEM NAME* FROM THEIR WORKSTATIONS IN ROOM 5678." The risks were evaluated in the following security domains:

- Managerial,
- Technical,
- Operational, and
- Administrative

IF ANY SITE VISITS WERE CONDUCTED, EXPLAIN HERE. FOR EXAMPLE, "SITE VISITS AT DEPARTMENT HEADQUARTERS WERE RESTRICTED TO ROOM 1234 WHERE THE EDNET SERVER AND THE RAS ARE LOCATED, AND OEF OFFICES IN 5678. TO OBSERVE REMOTE ACCESS CAPABILITY, THE HOMES OF TWO USERS WERE VISITED TO REVIEW THE DIAL-UP NETWORKING AND VIRTUAL PRIVATE NETWORKING (VPN) PROCESS."

1.4 REPORT ORGANIZATION

This document is divided into four sections and an appendix. Section 1 is the introduction. The remainder of the document consists of the following sections:

- Section 2 provides a description of the risk assessment methodology used by INSERT CONTRACTOR NAME;
- Section 3 describes the characteristics of INSERT SYSTEM NAME including the hardware, software, connectivity, data, and system users; and
- Section 4 provides an analysis of the findings in the management, technical, operation, and administrative security domains.

Additionally, the document contains an appendix that provides the details of the risk assessment.

2.0 RISK ASSESSMENT APPROACH

Risk was evaluated qualitatively, meaning that numerical values were not assigned. Instead a rating of high, medium, or low was provided. The INSERT CONTRACTOR NAME risk assessment methodology involved three major steps that are described below.

- Step 1 – Determine System Boundary
- Step 2 – Gather Information
- Step 3 – Conduct Risk Assessment.

The methodology used to perform the risk assessment for INSERT SYSTEM NAME was developed by INSERT CONTRACTOR NAME with reference to the following guidelines:

- National Institute of Standards and Technology (NIST) Special Publication 800-30, *Risk Management Guide for Information Technology Systems* (Draft).
- Office of Management and Budget (OMB) Circular A-130 "Security of Federal Automated Information Systems."

The level of risk was assessed by evaluating all collected risk-related attributes regarding threats, vulnerabilities, assets and resources, current controls, and the associated likelihood that a vulnerability could be exploited by a potential threat and the impact (e.g., magnitude of loss resulting from such exploitation).

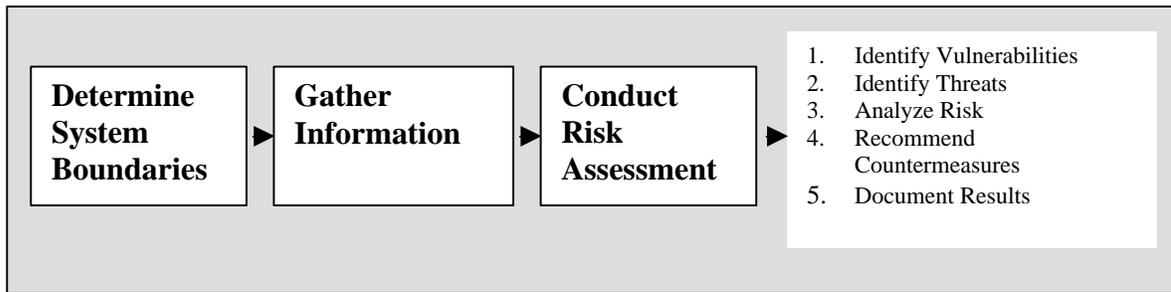


Figure 1: Risk Assessment Approach

2.1 STEP 1 – DEFINE SYSTEM BOUNDARY

The system boundaries, which determine the risk assessment scope, were restricted to the INSERT SYSTEM NAME. DESCRIBE HOW SYSTEM BOUNDARY WAS ESTABLISHED. FOR EXAMPLE, "MEETINGS WITH THE OEF PRINCIPAL OFFICER AND THE DEPARTMENT'S CHIEF INFORMATION OFFICER ALONG WITH REVIEWING THE CURRENT SYSTEM DIAGRAMS LED TO A DETERMINATION OF THE BOUNDARIES."

2.2 STEP 2 – GATHER INFORMATION

INSERT CONTRACTOR NAME assessed the INSERT SYSTEM NAME based on the risk assessment team’s understanding of the operational environment and SFA and Department-wide information technology (IT) policies and guidelines. Information about INSERT SYSTEM NAME was gathered through INSERT METHODS USED TO GATHER INFORMATION. FOR EXAMPLE, " INTERVIEWS, SITE VISITS, DOCUMENTATION REVIEW, AND THE USE OF AN NETWORK-SCANNING TOOL."

2.2.1 Interviews

IF INTERVIEWS WERE CONDUCTED, INSERT A DESCRIPTION. FOR EXAMPLE, "TO COLLECT RELEVANT INFORMATION, *INSERT CONTRACTOR NAME* DEVELOPED A QUESTIONNAIRE ON IT SYSTEM MANAGEMENT AND OPERATIONS OF THE *INSERT SYSTEM NAME* AND SUPPORT PLATFORM. THE INTERVIEWS WERE CONDUCTED ON-SITE, VIA TELEPHONE, AND THROUGH EMAIL WITH THE FOLLOWING SFA MANAGEMENT AND TECHNICAL PERSONNEL:

- EDNET SERVER ADMINISTRATOR,
- SFA SYSTEM SECURITY OFFICER,
- SFA COMPUTER SECURITY OFFICER,
- SFA EXECUTIVE OFFICER,
- *INSERT SYSTEM NAME* USERS"

2.2.2 Site Visit

IF SITE VISITS WERE CONDUCTED, INSERT A DESCRIPTION. FOR EXAMPLE, "THE *INSERT CONTRACTOR NAME* TEAM TOURED THE COMPUTER ROOM WHICH HOUSES THE *INSERT SYSTEM NAME* HARDWARE, SOFTWARE AND DATA AT ROOMS 1234 AND 5678 AT ROB3 ON JULY 28, 2001 TO OBSERVE THE PHYSICAL AND ENVIRONMENTAL MEASURES PROVIDED FOR THE *INSERT SYSTEM NAME*. THE VISIT ALSO INCLUDED A DEMONSTRATION OF HOW THE SYSTEM IS ACCESSED AND ADMINISTERED, INCLUDING ADDING AND REMOVING DATA. *INSERT CONTRACTOR NAME* ALSO VISITED THE HOMES OF TWO SFA STAFF MEMBERS TO OBSERVE REMOTE CONNECTIONS VIA VIRTUAL PRIVATE NETWORK AND DIAL-UP NETWORKING."

2.2.3 Documentation

The team reviewed all relevant information security (INFOSEC) documents in order to develop a better understanding of *INSERT SYSTEM NAME*. Listed below are all system and organizational documents reviewed in support of the assessment:

- *INSERT SYSTEM NAME* Security Plan,
- 2001 NIST Self-Assessment,
- Recent IG, GAO Audits,
- *INSERT SYSTEM NAME* User's Guide,
- *INSERT SYSTEM NAME* Configuration Management Plan (CMP),
- SFA request for proposal (RFP) for development of *INSERT SYSTEM NAME*, and
- *INSERT ANY OTHER DOCUMENTATION REVIEWED FOR THIS RISK ASSESSMENT*.

2.2.4 Network Scanning

IF NETWORK SCANNING WAS CONDUCTED, INSERT A DESCRIPTION. FOR EXAMPLE, " THE TEAM USED A SCANNING TOOL TO DISCOVER ADDITIONAL VULNERABILITIES, OR VULNERABILITIES MISSED BY ANOTHER SCANNER, AND TO MINIMIZE THE IMPACT OF FALSE POSITIVES. THE EDNET HOST WAS SCANNED ON AUGUST 12, 2001 AND AGAIN ON AUGUST 20, 2001.

2.3 STEP 3 – CONDUCT RISK ASSESSMENT

The risk assessment encompassed the following subtasks:

- Compiling the Vulnerability List,
- Identifying and associating potential threats to vulnerabilities,
- Determining risks, and

- Developing countermeasure recommendations

The value of INSERT SYSTEM NAME is measured in terms of the criticality and sensitivity of a system and its data.

To assess risks to INSERT SYSTEM NAME, the INSERT CONTRACTOR NAME risk assessment team identified a list of potential vulnerabilities that could be exploited by natural, environmental, human, or administrative threats. Section 3 provides an analysis of the possible threats and threat agents that could exploit vulnerabilities in INSERT SYSTEM NAME.

Section 4 and appendix A presents the findings and includes a discussion of the threat and vulnerability pair, , impact and likelihood analysis, risk rating, and recommended countermeasures.

In order to determine risk the team identified the impact an exploited vulnerability would have on the system and the likelihood of the vulnerability being exploited. The following sections provide descriptions of vulnerabilities, impact, likelihood, and an overall risk matrix.

2.3.1 Documenting Vulnerabilities

Upon completion of the documentation reviews, testing, etc. we documented each identified vulnerability in Appendix A of the assessment. Once our list of vulnerabilities was complete, we categorized the identified vulnerabilities into the following four primary security areas

- Management Security,
- Operational Security,
- Technical Security, and
- Administrative Security

Based on NIST Special Publication 800-18, we determined to which category the vulnerability most appropriately belonged.

Management controls focus on the management of the IT security system and the management of risk for a system. They are techniques and concerns that are normally addressed by management. There was one finding in the area of management security.

The **operational** controls address security methods focusing on mechanisms primarily implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). Often, they require technical or specialized expertise and rely upon management activities as well as technical controls. There were a total of 3 findings in the area of operational security.

Technical controls focus on security controls that the computer system executes. The controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. There were a total of 4 findings in the area of technical security.

Administrative controls focus on regulatory and policy issues that do not fit easily into the other three categories. These controls reflect specifically mandated documentation, actions, or decisions a system owner must address to adequately implement security policy, both at the federal and department level.

2.3.2 Impact

Impact refers to the magnitude of potential harm that may be caused by threat exploitation. It is determined by the value of the resource at risk, both in terms of the information sensitivity and its importance to the Department’s mission (i.e., criticality). The criticality and sensitivity of both the system and data are useful guides for assessing the potential impact of an exploited vulnerability. The table below provides a general description of impact.

Impact	Description
High	May result in the <i>loss</i> of significant information, or information resources. May significantly disrupt or impede SFA’s mission or seriously harm its reputation or interest.
Medium	May result in the <i>loss of some</i> tangible assets, information, or information resources. May disrupt or harm the SFA mission or harm its reputation or interest.
Low	May result in the <i>loss of minimal</i> tangible assets, information, or information resources. May adversely affect the ChTS mission, reputation, or interest.

Table 1: Impact Description

To determine impact, we compared the INSERT SYSTEM NAME’s sensitivity and criticality.

- Sensitivity takes into account the Confidentiality, Integrity and Availability.
- Criticality is the system’s impact to the agency, and is rated at either Mission Critical, Important or Supportive

First we reviewed the sensitivity rating determined during the inventory review. For each identified vulnerability and associated threat, we determined which sensitivity category might have been impacted if the vulnerability was exploited. Certain threats did not impact every category; rather, only certain categories were impacted. For example, a denial of service attack may only impact availability, but confidentiality or integrity remained unaffected. In this case the sensitivity level was based solely upon your availability rating. Another example is the vulnerability of unencrypted data, where the threat may impact confidentiality and integrity, but not availability. In this case, we would choose the higher rating of confidentiality or integrity.

The criticality rating we used was extracted from the recent inventory review worksheet. After conducting a brief review of the rationale for our rating, we established the criticality rating of INSERT SYSTEM NAME to be INSERT MISSION CRITICAL, MISSION IMPORTANT OR MISSION SUPPORTIVE.

For each vulnerability/threat pair we took our sensitivity rating (High, Medium, Low) and our criticality rating (Critical, Important, Supportive) and input them into the matrix below to determine the impact rating. Our calculation of impact was calculated as follows:

- 1) Sensitivity: Confidentiality (H/M/L), Availability (H/M/L) Integrity (H/M/L) = Overall Rating: H/M/L
- 2) Criticality: Mission Critical, Important, Supportive
- 3) Impact: High, Medium Low

Sensitivity X Criticality = Impact.

	System Criticality		
Information Sensitivity	<i>Mission Critical</i>	<i>Mission Important</i>	<i>Mission Supportive</i>
<i>High</i>	High	High	Medium
<i>Medium</i>	High	Medium	Medium
<i>Low</i>	Medium	Medium	Low

Table 2: Impact Description

The results of our impact analyses are documented as part of the Risk Assessment Matrix found in Appendix A of this document.

2.3.3 Likelihood

Likelihood is determined by considering threats and vulnerabilities. The likelihood that vulnerability will be exploited by a threat can be assessed and described as High, Medium, or Low. Factors that govern the likelihood of threat exploitation include threat capability, the frequency of threat occurrence, and effectiveness of current countermeasures. Generally, the likelihood of a threat exploiting vulnerability can be described as presented in the table below.

Likelihood	Description
High	The capability of the threat is significant, and/or countermeasures to reduce the probability of threat exploitation are insufficient.
Medium	The capability of the threat is moderate, and implemented countermeasures lessen the probability of threat exploitation.
Low	The capability of the threat is limited, and countermeasures are in place effectively reducing the probability of threat exploitation.

Table 3 – General likelihood description

To assess the likelihood of a threat exploiting a vulnerability, we divided likelihood into two components: Threat Capability and Countermeasure Effectiveness. The matrix below illustrates the relationship of a threat or threat agent to the capabilities of the threat or threat agent, and the existing countermeasures employed to guard against the threat. For the purposes of these analyses, capabilities are defined as the inherent difficulty in acting out the threat regardless of any existing countermeasures.

Threats	Capabilities	Countermeasures
Natural	Location Based H/M/L	Building codes, cold sites
Environmental	History Based H/M/L	Back-ups, redundancies
Human	Access based H/M/L	Firewalls, guards, IDS, audit logs, RoB
Administrative	H	Documentation

Table 4 – Likelihood matrix

If a threat was determined to be of natural origin (i.e. tornado, hurricane, flood, etc), the capabilities of the threat were based upon the geographic location of the system (and therefore the vulnerability in question). For example, the threat of hurricanes in Florida is much greater than the threat of a hurricane in Oklahoma. Therefore, a system located in Florida would have a high likelihood of a hurricane occurring as opposed to Oklahoma. However, the inverse can be said for tornados in Oklahoma.

For purposes of our analyses, environmental threats were constrained to an historical perspective. For example, the question was asked, “How many times has the heating and cooling system ever failed in the past year?” If the answer is 0, the rating was low; 1-2, the rating was medium; 3 or more, the rating was high.

Because of the wide variety of human threat agents, determining the threat capabilities of a human agent depended on the vector of the threat. Essentially, human threats could be broken down into numerous subcategories, the most important for this exercise being external vs. internal, and network vs. physical. If the threat was an external agent using network access, the capability was rated as high due to the sheer volume of attempted network attacks against all government systems. If no external access was available, the network threat capability was reduced to medium due to the potential existence of disgruntled employees, unintentional errors, etc. If the threat was of a more physical nature (theft, vandalism, sabotage, etc.), the capability was rated by the difficulty in carrying out the attack.

Administrative threats, due to the constant reviews and audits conducted by the IG, GAO, OMB, and Departmental teams, were given a high capability rating. We assumed that our system’s administrative deficiencies would be discovered by at least one of these groups, requiring urgent compliance to the applicable standards or policies.

After determining the capability of the threat, we analyzed the existing countermeasures we employed to guard against the threat. For example, if our system was located in Florida, specific building codes would be established to protect against a hurricane. To measure the effectiveness of the system’s countermeasures, we used the following subjective scale.

- If our assessment indicated we employed numerous measures to combat the specific threat and were confident in the their effectiveness, we rated the countermeasures effectiveness as high.
- If our assessment indicated we did not do much to address this particular threat and found our countermeasures lacking or non-existent, we rated the countermeasures as low.
- If our assessment indicated a moderate level of controls, more than low and less than high, we rated the countermeasures as medium.

Once the threat capability and countermeasure effectiveness were assessed for each vulnerability/threat pair, we used the matrix below to determine the overall likelihood of the threat exploiting the vulnerability. The findings were documented in Appendix A of this risk assessment.

	Countermeasure Effectiveness		
Capability	High	Medium	Low
High	Medium	High	High
Medium	Low	Medium	Medium
Low	Low	Low	Low

Table 5: Likelihood Rating

2.3.4 Risk

After evaluating likelihood and impact, the risk assessment team employed a risk scale matrix with the ratings of high, medium, and low to determine the degree or level of risk to which a system, facility, or procedure might be exposed if a vulnerability were exploited by an associated threat. The level of risk equals the intersection of the likelihood and impact values. For example, suppose the likelihood level is High and the impact level is Low for the threat/vulnerability pair. Based on the risk matrix found below, there would be a Medium risk level.

Risk = Impact X Likelihood

	Likelihood		
Impact	<i>High</i>	<i>Medium</i>	<i>Low</i>
<i>High</i>	High	High	Medium
<i>Medium</i>	High	Medium	Low
<i>Low</i>	Medium	Low	Low

Table 6: Risk Rating

3.0 SYSTEM CHARACTERIZATION

3.1 SYSTEM OVERVIEW

LIST GENERAL PURPOSE OF SYSTEM, HARDWARE, HARDWARE LOCATION, SOFTWARE, SOFTWARE LOCATION. FINALLY, CONCLUDE THIS SECTION WITH LOGICALLY-ORIENTED NETWORK DIAGRAM.

3.2 SYSTEM INTERFACES

INSERT SYSTEM INTERFACE DESCRIPTION FROM INVENTORY WORKSHEET OR SYSTEM SECURITY PLAN. INCLUDE A DIAGRAM OF THE CONNECTION(S). IF FURTHER GUIDANCE IS NECESSARY, INCLUDE A DESCRIPTION SUCH AS, "THE INSERT SYSTEM NAME DOES NOT GIVE OR RECEIVE ANY DATA TO ANY OTHER MAJOR APPLICATION (MA) OR GSS. INSERT SYSTEM NAME RESIDES ON EDNET AS ITS GSS, BUT OTHERWISE DOES NOT INTERFACE WITH ANY OTHER SYSTEM. IT IS ACCESSED FROM LOCAL SFA WORKSTATIONS. SFA STAFF MAY ACCESS THIS DATABASE WHEN THEY CONNECT REMOTELY EITHER THROUGH ANALOG DIALUP TO THE RAS SERVER OR THROUGH THE VPN CONNECTION.

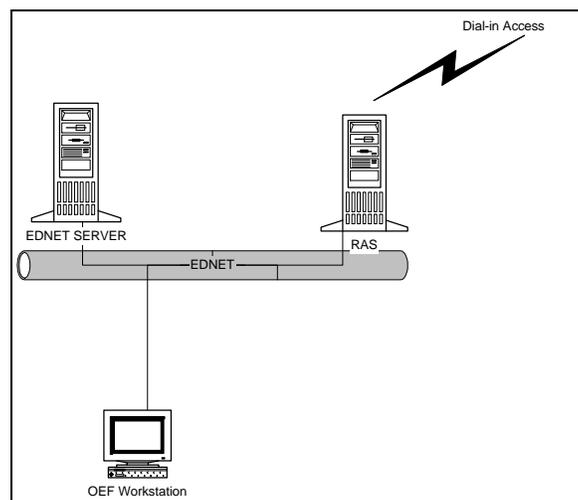


Figure 1: Connectivity

3.3 DATA

INSERT DESCRIPTION OF DATA FROM SYSTEM INVENTORY WORKSHEET. IF FURTHER GUIDANCE IS NECESSARY, INCLUDE A DESCRIPTION SUCH AS, “INSERT SYSTEM NAME DOES NOT CONTAIN ANY PRIVACY ACT INFORMATION OR PROPRIETARY DATA IN ITS TABLES. DATA STORED IN INSERT SYSTEM NAME INCLUDES SPECIFIC ATTRIBUTES ABOUT THE CHAIRS SUCH AS COLOR, BRAND, MODEL NUMBER, CATEGORY (ARM, SIDE, TABLE), AND FABRIC. INFORMATION DETAILING CHAIR LOCATION INCLUDING STAFF NAME, ROOM NUMBER, AND DATE ASSIGNED, IS ALSO STORED IN THE SYSTEM.”

3.4 SYSTEM AND DATA CRITICALITY AND SENSITIVITY

3.4.1 Criticality

INSERT CRITICALITY DESCRIPTION FROM INVENTORY WORKSHEET. IF MORE EXAMPLES ARE NEEDED, INCLUDE A DESCRIPTION SUCH AS, "SYSTEM NAME DOES NOT CONTAIN ANY SENSITIVE DATA AND THE FAILURE OF SYSTEM NAME WOULD NOT PRECLUDE SFA FROM ACCOMPLISHING CORE BUSINESS OPERATIONS IN THE SHORT TO LONG TERM (FEW HOURS TO FEW WEEKS). HOWEVER, FAILURE OF THE SYSTEM WOULD HAVE AN IMPACT ON THE EFFECTIVENESS OR EFFICIENCY OF DAY-TO-DAY OPERATIONS. CONSEQUENTLY THE SYSTEM NAME DATABASE IS CONSIDERED **MISSION SUPPORTIVE**."

3.4.2 Sensitivity

The criteria used to measure a system’s sensitivity include confidentiality, integrity, and availability. The sensitivity areas for INSERT SYSTEM NAME are described below.

3.4.2.1 Confidentiality:

INSERT CONFIDENTIALITY DESCRIPTION FROM INVENTORY WORKSHEET. IF MORE EXAMPLES ARE NEEDED, INCLUDE A DESCRIPTION SUCH AS, “**LOW**. THERE IS NO PRIVACY ACT OR PROPRIETARY DATA TO PROTECT. NO VENDOR OR COST INFORMATION IS TRACKED ON THE CHAIRS, ONLY BRAND AND MODEL. IF A NON-AUTHORIZED PERSON READ DATA THAT THEY ARE NOT “ALLOWED” TO SEE, ADMINISTRATIVE ACTION (SUCH AS SUSPENSION OR A LETTER OF UREPRIMAND) WOULD BE THE MOST SEVERE CONSEQUENCE. IF THE CHAIR RATINGS WERE DISCOVERED BY OUTSIDE CHAIR COMPETITORS, THE FINANCIAL IMPACT WOULD BE UNDER 100,000 DOLLARS.”

3.4.2.2 Integrity:

INSERT INTEGRITY DESCRIPTION FROM INVENTORY WORKSHEET. IF MORE EXAMPLES ARE NEEDED, INCLUDE A DESCRIPTION SUCH AS, "**MEDIUM**. THE DATA MAINTAINED ON THE CHAIR RATINGS DOES AFFECT RECOMMENDATIONS FOR PARTICULAR CHAIRS. SINCE ENTIRE SCHOOL DISTRICTS USE THESE RECOMMENDATIONS, THE FINANCIAL IMPACT OF MANIPULATED RATINGS COULD BE BETWEEN \$150,000 AND \$300,000, BUT LESS THAN A MILLION DOLLARS. ANYONE INVOLVED WITH SUCH DATA MANIPULATION WOULD POSSIBLY BE SUED BUT NOT SENT TO JAIL."

3.4.2.3 Availability:

INSERT AVAILABILITY DESCRIPTION FROM INVENTORY WORKSHEET. IF MORE EXAMPLES ARE NEEDED, INCLUDE A DESCRIPTION SUCH AS, "**LOW**. THE REPORTS ARE MUCH EASIER TO PREPARE WITH THE DATABASE AND IT WOULD BE VERY INCONVENIENT IF THE DATABASE WERE UNAVAILABLE. HOWEVER, MANUAL INSPECTION COULD BE USED. THE CONSEQUENCES OF THE DATABASE BEING UNAVAILABLE WOULD PROBABLY NEVER EVEN BE ADMINISTRATIVE. THE EXTRA MANPOWER REQUIRED TO MANUALLY PREPARE THE REPORTS WOULD BE LESS THAN \$100,000 SINCE AT WORST, A CONTRACTOR COULD BE HIRED TO PREPARE THE MOST IMPORTANT REPORTS FOR \$75,000.

The table below summarizes the sensitivity levels. The overall system sensitivity level is determined by the highest value in the INSERT SYSTEM NAME Level column. Therefore, the sensitivity level for INSERT SYSTEM NAME is **INSERT OVERALL SYSTEM SENSITIVITY LEVEL**.

Sensitivity Class	INSERT SYSTEM NAME Level
Confidentiality	INSERT LEVEL
Integrity	INSERT LEVEL
Availability	INSERT LEVEL

Table 7: Sensitivity Rating

3.5 USERS

INSERT DESCRIPTION OF SYSTEM USERS INFORMATION FOR THIS SECTION SHOULD BE LOCATED IN THE SYSTEM’S SECURITY PLAN. IF MORE GUIDANCE IS NECESSARY, INCLUDE A SIMILAR DESCRIPTION AS FOLLOWS, “ONLY EDNET USERS MAY GAIN ACCESS TO SYSTEM NAME SINCE IT IS LOCATED ON AN EDNET SERVER. THERE IS AN ADDITIONAL LOGON UNIQUE TO THE DATABASE. THERE ARE THREE TYPES OF ACCESS ALLOWED:

- ADMINISTRATIVE WHICH PROVIDES TOTAL CONTROLS,

- EXECUTIVE WHICH ALLOWS ACCESS TO ALL REPORTS AND THE ABILITY TO UPDATE KEY FIELDS DEALING WITH THE ASSIGNMENT OF CHAIRS, AND
- BASIC WHICH ALLOWS ACCESS TO MOST, BUT NOT ALL FORMS, AND THE ABILITY TO UPDATE THE FIELDS RELATING TO INFORMATION ABOUT ALREADY ASSIGNED CHAIRS.”

4.0 THREAT STATEMENT

4.1 THREAT SOURCES

A threat is any instance that could disrupt the ability of INSERT SYSTEM NAME to fulfill its purpose. The four major categories of threats stem from nature, inadequate environmental controls, acts by individuals, and administrative. Examples are categorized and listed in the table below.

Natural Disaster				
Storm damage (e.g., flood, rain, snow, tornado)	Fire	Lightning strikes	Earthquakes	
Environmental Control Failures				
Long-term power failure	HVAC Failures	Pollution	Liquid leakage	Biological/chemical terrorism
Human Acts				
Assault on an employee	Arson	Blackmail		
Bomb/terrorism	Browsing of privacy and proprietary information	Civil disorder		
Corrupted data input	Distributed Denial of Service	Economic exploitation		
Falsified data input	Fraud	Hacking		
Impersonation	Interception	Labor dispute/strike		
Malicious code	Negligence/human error	Packet-sniffing		
Password-guessing (e.g., dictionary attack, brute force attack)	Web defacement	Sabotage/vandalism		
Spoofing	System tampering	Theft		
Unauthorized disclosure and modification of sensitive information	Virus implant			
Administrative threats				
Inspector General	GAO	OMB		
Department	Congress	NIST		

Table 8: Threat Sources

4.2 THREAT ACTIONS

SFA believes human threat agents or individuals—authorized and unauthorized—to be the biggest potential threats to its systems and its data. Humans could cause intentional or unintentional damage to almost any SFA system, potentially impairing the ability of it systems to operate effectively. Possible human threat agents include:

- Insiders, disgruntled employees, dishonest employees, malicious persons,
- Authorized users (e.g., privileged system users, such as DBA, system administrator, computer operator; and unprivileged system users and application users),
- Terminated employees, including retired, resigned, or fired employees,
- Contractors and subcontractors (e.g., cleaning crew, technical support personnel, developers, and computer and telephone service repair staff),
- Foreign chair companies or foreign governments with an interest in the information held in the ChTS, and
- Unauthorized users, who may use hacking or penetration techniques against an SFA system or EDNet with the malicious intent of disrupting normal operations and causing harm to a system (e.g., computer criminals, terrorists, hackers, intruders, Internet users, perpetrators).

5.0 FINDINGS

Appendix A of this document represents the findings of the risk assessment performed on INSERT SYSTEM NAME. An observation resulted when vulnerability was identified with a threat that could exploit the vulnerability. Several methods were employed to identify vulnerabilities to the system from documentation reviews to vulnerability scans. Each of the observations is listed and numbered singularly in the appendix. The presentation of each observation consists of the following:

- Prioritized number of the observation,
- Detailed description of the vulnerability,
- A list of the threat(s) identified in the NEHA category,
- An impact assessment of the likelihood that a vulnerability will be exploited by a threat and the impact on INSERT SYSTEM NAME of successful exploitation,
- An assessment of the level of risk to INSERT SYSTEM NAME based on the threat and vulnerability assessment, and
- A recommendation of countermeasures that would reduce or eliminate the risk.

Appendix A is in Microsoft Excel format and can be imported into this document if desired. However, this action is not required.