Controlled

Unclassified

Information

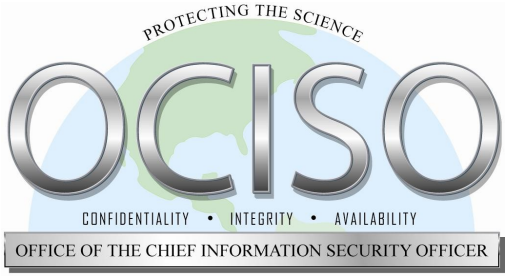
(CUI)

(When Filled IN)

Centers for Disease Control and Prevention

<System Name>

Draft Risk Assessment Report



Submitted to Tom Madden, CISO
DHHS/CDC/CIO/OCISO
4770 Buford Highway K-81
Atlanta, GA 30329

Submitted: , 2007

Version Control

Date	Author	Version

EXECUTIVE SUMMARY

The Centers for Disease Control and Prevention (CDC) recognizes the best, most up-to-date health information is without value unless it is pertinent and accessible to the people it is meant to serve. Lockheed Martin Information Technology has been tasked to conduct a risk assessment of the **<System Name and Acronym>** for the purpose of certification and accreditation (C&A) of **<System Name>** under *DHHS Information Security Program Policy.* This Risk Assessment Report, in conjunction with the System Security Plan, assesses the use of resources and controls to eliminate and/or manage vulnerabilities that are exploitable by threats internal and external to CDC. The successful completion of the C&A process results in a formal Authorization to Operate of **<System Name>**.

The scope of this risk assessment effort was limited to the security controls applicable to the **<System Name>** system's environment relative to its conformance with the minimum *DHHS Information Technology Security Program: Baseline Security Requirements Guide*. These baseline security requirements address security controls in the areas of computer hardware and software, data, operations, administration, management, information, facility, communication, personnel, and contingency.

The **<System Name>** risk assessment was conducted in accordance with the methodology described in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, *Risk Management Guide for Information Technology Systems*. The methodology used to conduct this risk assessment is qualitative, and no attempt was made to determine any annual loss expectancies, asset cost projections, or cost-effectiveness of security safeguard recommendations.

The risk assessment of **<System Name>** identified (?#?) vulnerabilities in the areas of Management, Operational and Technical Security. Vulnerabilities are weaknesses that may be exploited by a threat or group of threats. These vulnerabilities can be mitigated by (?#?) recommended safeguards. Safeguards are security features and controls that, when added to or included in the information technology environment, mitigate the risk associated with the operation to manageable levels. (?#?) vulnerabilities were rated **High**, (?#?) were rated **Moderate** and (?#?) were rated as **Low**. A complete discussion of the vulnerabilities and recommended safeguards are found in Section 6 of this report.

The overall **<System Name>** system security categorization is rated as <**Low, Moderate, High**> in accordance with Federal Information Processing Standards 199 (FIPS 199).

The E-Authentication Assurance Level (EAAL) was rated as (EAAL 1,2,3,4).

The following table provides an overview of the vulnerabilities and recommended safeguards for **<System Name>.** The vulnerabilities are listed by risk level.

<System Name> Risk Matrix

Vulnerability	Risk Level (High, Moderate, Low)	EAAL Transaction #	EAAL (1,2,3,4)	Recommended Safeguard
V-1.	Low	N/A	N/A	S-1.
V-2.	Moderate	2	2	S-2.

If the safeguards recommended in this risk assessment are not implemented, the result could be modification or destruction of data, disclosure of sensitive information, or denial of service to the users who require the information on a frequent basis.

Table of Contents

1 INTRODUCTION

1.1 Purpose

The purpose of this risk assessment is to evaluate the adequacy of the <**System Name and Acronym**> security. This risk assessment provides a structured qualitative assessment of the operational environment. It addresses sensitivity, threats, vulnerabilities, risks and safeguards. The assessment recommends cost-effective safeguards to mitigate threats and associated exploitable vulnerabilities.

1.2 Scope

The scope of this risk assessment assessed the system's use of resources and controls (implemented or planned) to eliminate and/or manage vulnerabilities exploitable by threats internal and external to the Centers for Disease Control and Prevention (CDC). If exploited, these vulnerabilities could result in:

- Unauthorized disclosure of data
- Unauthorized modification to the system, its data, or both
- Denial of service, access to data, or both to authorized users

This Risk Assessment Report evaluates the **confidentiality** (protection from unauthorized disclosure of system and data information), **integrity** (protection from improper modification of information), and **availability** (loss of system access) of the system. Recommended security safeguards will allow management to make decisions about security-related initiatives.

1.3 Mission

The **<System Name>** mission is to …

2 RISK ASSESSMENT APPROACH

This risk assessment methodology and approach was conducted using the guidelines in NIST SP 800-30, *Risk Management Guide for Information Technology Systems*. The assessment is broad in scope and evaluates security vulnerabilities affecting confidentiality, integrity, and availability. The assessment recommends appropriate security safeguards, permitting management to make knowledge-based decisions about security-related initiatives. The methodology addresses the following types of controls:

- **Management Controls:** Management of the information technology (IT) security system and the management and acceptance of risk
- **Operational Controls:** Security methods focusing on mechanisms implemented and executed primarily by people (as opposed to systems), including all aspects of physical security, media safeguards, and inventory controls
- **Technical Controls:** Hardware and software controls providing automated protection to the system or applications (Technical controls operate within the technical system and applications.)

2.1 Risk Assessment Process

This section details the risk assessment process performed during this effort. The process is divided into pre-assessment, assessment, and post-assessment phases.

2.1.1 Phase I – Pre-Assessment

Step 1: Define the Nature of the Risk Assessment

This initial risk assessment provides an independent review to help CDC determine the appropriate level of security required for the system to support the development of a System Security Plan for **<System Name>**. The review also provides the information required for the Chief Information Security Officer (CISO) and Designated Approving Authority (DAA (also known as the Authorizing Official)) to make an informed decision about authorizing the system to operate. The risk assessment is based on interviews, documentation and, as necessary, some automated technical review.

Step 2: Data Collection

The data collection phase included identifying and interviewing key personnel within the organization and conducting document reviews. Interviews focused on the operating environment. Document reviews provided the risk assessment team with the basis on which to evaluate compliance with policy and procedure.

Step 3: Templates

The following templates were used by the risk assessment team and are included in the appendices:

- **NIST SP 800-53, Revision 2, Security Baseline Worksheet:** Completed by the analysts using information extracted from questionnaires and interviews.

- **Risk Calculation Worksheet:** Converts the raw vulnerabilities into risks based on the following methodology:
  - Categorizing vulnerabilities
  - Pairing with threat vectors
  - Assessing the probability of occurrence and possible impact
  - E-authentication assessment
  - Determining e-authentication EAAL threat vectors
- **Risk Mitigation Worksheet:** Lists the risks and the associated recommended controls to mitigate these risks for the Business Steward to review. The Business Steward is responsible for formally accepting each recommended control or rejecting it and providing an alternative. For each rejected recommendation, the CDC Business Steward must note that the risk is to be accepted as residual risk. The Certification Agent (CA) (for the CDC this is the CDC CISO) will, at the same time or shortly thereafter, evaluate the Business Steward's selections and agree to each (e.g., accepting the risks and chosen recommended controls) or will negotiate an alternative mitigation, while reserving the right to override the Business Steward's decision and incorporate the proposed recommended control into the Plan of Action and Milestones (POA&M).

2.1.2 Phase II – Assessment

Step 1: Document Review

The assessment phase began with the review of documents provided by the members of the CDC **<System Name>** system team. Detailed interviews with members of the CDC **<System Name>** system team allowed completion of the system questionnaire and identification of specific threats inadequately identified in the Enterprise Threat Statement.

Step 2: System Characterization

In this step, the analyst defined the boundaries of the IT system, along with the resources that constitute the system, its connectivity, and any other elements necessary to describe the system. Dependencies were clarified. Sensitivity of the system and data was discussed in the final section of the characterization.

Step 3: Threat Identification

The risk assessment team used the CDC Enterprise Threat Statement and the NIST SP 800-30 as a basis for threat identification. Through the interview process, it also identified "most likely" system and location-specific threats.

Step 4: Vulnerability Identification

In this step, the risk assessment team developed a list of system vulnerabilities (flaws or weaknesses) that could be exploited by the potential threat vectors. The NIST SP 800-53, Revision 2, Security Baseline Worksheet (Appendix B of the Risk Assessment Report)

documents vulnerabilities extracted from interviews and documents, and lists them by category.

Step 5: Risk Determination (Calculation/Valuation)

In this step, the risk assessment team determined the degree of risk to the system. In some cases, a series of vulnerabilities combined to create the risk. In other cases, a single vulnerability created the risk. The determination of risk for a particular threat source was expressed as a function of the following:

- **Likelihood Determination:** The following governing factors were considered when calculating the likelihood of the probability that a potential vulnerability might be exploited in the context of the associated threat environment:
  - Threat source motivation and capability
  - Nature of the vulnerability
  - Existence and effectiveness of current controls

The following table defines the likelihood determinations.

Table (?). Likelihood Definition

Level	Likelihood Definition
High	The threat source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Moderate	The threat source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

- **Impact Analysis:** The next major step in measuring level of risk was to determine the adverse impact resulting from successful exploitation of a vulnerability. The adverse impact of a security event can be described in terms of loss or degradation of any, or a combination of any, of the following three security goals:
  - Loss of Confidentiality – Impact of unauthorized disclosure of sensitive information (e.g., Privacy Act).
  - Loss of Integrity – Impact if system or data integrity is lost by unauthorized changes to the data or system.
  - Loss of Availability – Impact to system functionality and operational effectiveness.

Table (?). Impact Definition

Magnitude of Impact	Impact Definition
High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organizations mission, reputation, or interest; or (3) may result in human death or serious injury.
Moderate	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm or impeded an organization's mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources; (2) may noticeably affect an organization's mission, reputation, or interest.

- **Risk Determination:** The following were used to assess the level of risk to the IT system:
  - The likelihood of a given threat source's attempting to exercise a given vulnerability.
  - The magnitude of the impact should a threat-source successfully exercise the vulnerability.
  - The adequacy of planned or existing security controls for reducing or eliminating risk.

The following table provides a definition for the risk levels**.** These levels represent the degree or level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised.

Table (?). Risk Level Definition

Magnitude of Impact	Risk Level Definition
High	There is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Moderate	Corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	The system's Authorizing Official must determine whether corrective actions are still required or decide to accept the risk.

Step 6: Risk Mitigation Recommendations

During this step of the process, controls that could mitigate or eliminate the identified risks, as appropriate to the organization's operations, were provided. The goal of the recommended controls is to reduce the level of risk to the IT system and its data to an acceptable level. The risk assessment team considered the following factors when recommending controls and alternative solutions to minimize or eliminate identified risks:

- Sensitivity of the data and the system
- Effectiveness of recommended options
- Legislation and regulations
- Organizational policy
- Operational impact
- Safety and reliability

The recommendations were the results of the risk assessment process, and provide a basis by which the CISO and Authorizing Official can evaluate and prioritize controls. The Business Steward will work with the CISO to negotiate the implementation of the recommended controls. At this point, the System Steward can negotiate with the CISO to accept the recommendations for risk mitigation, provide alternative suggestions, or reject the recommendations and accept the risk as residual risk. Their joint decision will form the basis of the POA&M.

2.1.3 Phase III – Post Assessment

Step 1: Risk Mitigation

The completed POA&M is the product from the preparation of the Risk Mitigation Worksheet and specific remedial recommendations to mitigate risk. Because the elimination of all risk is usually impractical, senior management and business stewards should assess control recommendations, determine the acceptable level of residual risk, and implement those mitigations with the most appropriate, effective, and highest payback.

Step 2: Ongoing Monitoring

The agreed-upon milestones to mitigate the risks are reportable to the Office of Management and Budget (OMB) and the POA&M is the reporting vehicle. The POA&M will be used by the CISO to monitor the successful completion of the milestones.

3 SYSTEM CHARACTERIZATION

3.1 System Stewards and Designated Approving Authority

Example:

*The **<System Name>** system became operational in January 2002 after being renamed from Acquisition Management Automation System (AMAS). It is continuously updated and is presently maintained by System Stewards (Table ?) in both the Management Information Systems Branch (MISB) and Procurement Grants Office (PGO).*

The following is contact information for **<System Name>** System Stewards and DAA.

Table ?. System Stewards and Designated Approving Authority (DAA)

	Business Steward	Security Steward	DAA
Name			
Title			
Address			
Phone			
E-mail			

3.2 Functional Description

Example:

The **<System Name>** system maintains information on the CDC's contracts, bids for services, procurement, and bid award data. Bidding information from contractors is kept private until a contract is awarded.

The **<System Name>** system is a client/server package that enables processing of both large contracts and simplified acquisition procurements (SAP). This Government Off-the-Shelf (GOTS) software package has replaced the Small Purchases Processing System (SPPS) and the Automated Receiving System (ARS).

The system was originally developed for the Department of Defense, but was customized for CDC by the BayTech Consulting Group of Annapolis, MD, between 1998 and 2003. Currently, CDC has a contract with DB Consulting Group on site at PGO for further development and maintenance of the system as its full functionality is realized. The original system name, AMAS, was changed to **<System Name>** to reflect functionality added for CDC.

<System Name> is a stand alone system that has no current real-time interfaces. **<System Name>** has the following batch interfaces:

3.3 System Environment

[Example: The **<System Name>** system environment is a client/server environment consisting of a Microsoft (MS) Structured Query Language (SQL) database built with PowerBuilder programming code. **<System Name>** contains production data files, application code, and executables. The production data files, consisting of stored procedures and tables, reside on a Clarion storage area network (SAN) attached to a Dell server running on Windows 2000 and MS SQL 2000 operating systems. The application code resides on a different Dell server running on Windows 2000. Both servers are housed in the Building 16 Data Center at the CDC Clifton Road campus in Atlanta, GA. The **<System Name>** executables reside on a fileserver running Windows 2000 or a local workstation depending upon the location and job functionality.

Users are physically located in multiple locations (multiple campuses in Atlanta, Cincinnati, Pittsburgh, Morgantown, Ft. Collins, Denver, Anchorage, Research Triangle Park, and San Juan). Their desktop computers are physically connected to a wide area network (WAN). Some users connect via secured dial-up/DSL connection using a Citrix server. Normally, a user connects to an application server in their city that hosts the **<System Name>** application, and to the shared database server located in Atlanta. All CIOs throughout CDC/ATSDR are users of **<System Name>]**.

Insert system diagram(s)

Figure 1. <System Name> Diagram

Table ? lists host characterization components for the **<System Name>** production system.

Table ?. <System Name> Host Characterization Components

Host Name	Location	Status	IP Address	Platform	Software	Comments
Example: Aop-irm-msb2	Clifton	Operational	Not provided	Windows	MS Windows 2000 Server Power-builder	

3.4 System Users

[Example: The primary **<System Name>** users are customers in PGO; however, **<System Name>** customers also include the CDC Centers, Offices, and Chief Information Officers (CIOs). The **<System Name>** system users are listed in Table ?; details include the **<System Name>** system user's name (title), description and responsibilities, and the stakeholders that represent each user's interest in the system].

Table ?. <System Name> System Users

User Category	Access Level Read / Write/Full	Number (Estimate)	Home Organization	Geographic Location
Example: Developers	Read/Write	10	ABC Group	Atlanta

3.5 System Dependencies

List specific dependencies

Beyond these dependencies, a set of common dependencies was defined to enable boundary definition. A dependency is a telecommunication or information technology interconnection or resource on which the system under review relies for processing, transport, or storage. The relationship between the system in question and the dependencies can directly affect the confidentiality, integrity, or availability of the system or its data. Whenever a system has a dependency, the system inherits the intrinsic risks of the dependent asset. The following CDC information technology resources can be considered dependencies:

- CDC Enterprise Policies
- CDC Enterprise Mid-Tier Data Center
- CDC Network Infrastructures:
  - Center or Information Technology Services Office (ITSO) Local Area Networks
  - Atlanta Metropolitan Area Network
  - CDC Wide Area Network
  - Internet Connectivity
- DMZ Connectivity
- CDC Enterprise Security Services:
  - CDC Border Firewall
  - CDC Border Router Access Control Lists
  - Network-Based Intrusion Detection Systems

E-Mail Gateway Virus Scanning and Attachment Removal

RSA SecurID Authentication System

- Technical Vulnerability Scanning Service (Most Commonly Used for Hosts Deployed to the DMZ)
- CDC Computer Room Staff, Physical, and Environmental Controls
- CDC Exchange Services:

  Enterprise E-Mail Gateway Infrastructure with Gateway Virus Protection

  ITSO or Center Managed Local E-Mail Stores with Server Virus Protection

  Remote Access Web Mail Services with RSA SecurID Authentication
- CDC Enterprise Continuity of Operations and Disaster Recovery Planning
- CDC Enterprise Mainframe
- CDC Enterprise Windows Domain/Active Directory Environment

3.6 Supported Programs and Applications

The following systems depend on **<System Name>** to perform or fulfill their function:

3.7 Information Sensitivity

This section provides a description of the types of information handled by **<System Name>** and an analysis of the sensitivity of the information. The sensitivity of the information stored within, processed by or transmitted by **<System Name>** provides a basis for the value of the system and is one of the major factors in risk management.

FIPS 199 establishes three potential impact levels (Low, Moderate, High) for each of the security objectives (confidentiality, integrity, and availability). The impact levels focus on the potential impact and magnitude of harm that the loss of confidentiality, integrity, or availability (C/I/A) would have on CDC's operations, assets, or individuals. FIPS 199 recognizes that an information system may contain more than one type of information (e.g., privacy information, medical information, financial information), each of which is subject to security categorization. Section 3.8.1 discusses the security categorization/ information type(s) for **<System Name>**.

3.7.1 Security Categorization/Information Type(s)

The security category of an information system that processes, stores, or transmits multiple types of information should be at least the highest impact level that has been determined for each type of information for each security objective of C/I/A. The following table depicts the security category/information type for **<System Name>** as identified in the **<System Name>** Risk Assessment Report.

Table (?). <System Name> Information Type

Information Type	NIST SP 800-60 Reference	Confidentiality Low/Moderate/ High	Integrity Low/Moderate/ High	Availability Low/Moderate/ High
Overall Rating				

Note: If C/I/A ratings differ from NIST SP 800-60, provide justification and obtain approval from OCISO.

3.7.2 Sensitivity

The following table provides the definitions for C/I/A ratings for **<System Name>**.

Table (?). Confidentiality, Integrity, and Availability Defined

Security Objective	Low	Moderate	High
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protection personal privacy and proprietary information [44 USC, SEC. 3542]	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 USC, SEC. 3542]	The modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 USC, SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

The sensitivity designation of information processed by **<System Name>** is **(High, Moderate, Low).** This **(High, Moderate, Low)** designation is based upon the C/I/A designation of the information type for **<System Name>**.

3.7.3 Protection Requirements

Both information and information systems have distinct life cycles. It is important that the degree of sensitivity of information be assessed by considering the requirements for the C/I/A of the information: the need for system data to be kept confidential; the need for the data processed by the system to be accurate, and the need for the system to be available. Confidentiality focuses on the impact of disclosure of system data to unauthorized personnel. Integrity addresses the impact that could be expected should system data be modified or destroyed. Availability relates to the impact to the organization should use of the system be denied.

3.7.4 Protection Requirement Findings[1]

- **Confidentiality:** *[Example:* **<System Name>** *contains sensitive information that could identify a survey participant. This data requires protection from unauthorized disclosure. If information contained in* **<System Name>** *were released to the public it could result in a loss of public confidence in the survey, affect participation, and cause a great deal of embarrassment to the CDC*]. Therefore, the unauthorized disclosure of **<System Name>** information could be expected to have a (**limited, serious, or severe**) adverse effect on organizational operations, organizational assets, or individuals and the information and protection measures are rated as **(Low, Moderate, High)**.
- **Integrity:** *[Example:* **<System Name>** *collects and processes health and nutritional information annually from a representative sample of the U. S. population. Because public health trends and policies depend on the accuracy of the data collected, unauthorized and unanticipated modification would seriously reduce the accuracy of the survey results]*. Therefore, the unauthorized modification of **<System Name>** information could be expected to have a (**limited, serious, or severe**) adverse effect on organizational operations, organizational assets, or individuals and the information and protection measures are rated as **(Low, Moderate, High)**.
- **Availability:** *[Example: If* ***<System Name>*** *were unavailable for even a short period of time, it would have an immediate impact and would affect the efficiency with which <System Name> typically operates]*. Therefore, the unavailability of **<System Name>** information could be expected to have a (**limited, serious, or severe**) adverse effect on organizational operations, organizational assets, or individuals and the information and protection measures are rated as **(Low, Moderate, High)**.

[1]Low – a limited adverse effect
Moderate – a serious adverse effect
High – a severe or catastrophic adverse effect

4 THREAT STATEMENT

4.1 Overview

NIST SP 800-30 describes the identification of the threat, the threat source and threat action for use in the assessment process. The following is a definition for each:

- **Threat** – The potential for a particular threat-source to successfully exercise a particular vulnerability. *(Vulnerability is a weakness that can be accidentally triggered or intentionally exploited)*
- **Threat Source** – Any circumstance or event with the potential to cause harm to an IT system. The common threat sources can be natural, human or environmental.
- **Threat Action** – The method by which an attack might be carried out (e.g., hacking, system intrusion).

4.2 Enterprise Threat Vector

- **Acts of Nature.** Earthquakes, rain, wind, ice, etc., that threaten facilities, systems, personnel, utilities, and physical operations.
- **Hazardous Conditions.** Fire, chemical and nuclear spills, biological events, structural instability, etc., that threaten facilities, systems, personnel, and operations. May be the result of natural events, environmental control failures, human errors, and/or violent acts.
- **Dependency Failures.** Failure of a system or service outside the direct control of the system owners that harms the system and/or affects its ability to perform. Also includes system worker termination and reassignment actions. Examples include utility failures, downstream processing failures, system administrator or subject matter expert job termination, or the failure of a service or control owned by another part of the organization.
- **System and Environmental Failures.** Failure of a computer, device, application, communication service, or environmental or protective control that disrupts, harms, or exposes the system to harm. Examples include system hardware failures, environmental control failures, and software or data corruption.
- **Violent Acts of Man.** Physical attack or threat of attack on a national, regional, or local level that directly impacts the system and/or its personnel or that results in indirect harm or dependency failure.
- **Errors and Omissions.** Accidental or ill-advised actions taken by personnel (typically insiders) that result in unintended physical damage, system disruption, and/or exposure.
- **Insider Attack.** Actions taken by insiders to harm the organization and its personnel, systems, and/or data and/or that of other parties. Examples include system compromise, escalation of privileges, electronic eavesdropping, password guessing, denial of service, and social engineering.

- **Insider Abuse and Unauthorized Acts.** Unauthorized, illegal, or inappropriate insider acts that cause disruption and/or harm. Although these actions are intentional, computing resources are typically the vehicle used to commit the act rather than its target. Examples include sharing or distribution of copyrighted material, invasion of privacy, exploration of unauthorized computer systems, use of computing resources to harass others, and disregard for security controls.
- **External Attack.** Actions taken by outside parties seeking to harm the organization, its personnel, systems, and/or data and/or that of other parties. Examples include system compromise, data and account harvesting, defacement, computer crime, password guessing, denial of service, and social engineering.
- **Autonomous Systems and Malicious Code.** Automated actions taken by program code or systems that result in harm to the organization, its systems, and/or its data and/or that of other parties. Examples include viruses, worms, and artificial intelligence control or response systems.
- **Physical Intrusion and/or Theft.** Facility compromise and/or theft of physical resources (data, hardcopy output, laptops, systems, access tokens, passwords, etc.) that could directly or indirectly result in harm to the organization or the system.
- **Legal and Administrative Actions.** Actions taken by law enforcement, regulatory, administrative, and/or other parties as a result of illegal acts and failures in due diligence and/or due care, or in seeking recompense for damages incurred by others. Examples include regulatory penalties, criminal and civil proceeding.

5 E-AUTHENTICATION

5.1 Overview

NIST SP 800-63 describes the categories of harm and impact as:

- Inconvenience, distress, or damage to standing or reputation
- Financial loss or agency liability
- Harm to agency programs or public interests
- Unauthorized release of sensitive information
- Personal safety
- Civil or criminal violations

Required assurance levels for electronic transactions are determined by assessing the potential impact of each of the above categories using the potential impact values described in FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems." The three potential impact values are:

- Low impact
- Moderate impact
- High impact

The next section defines the potential impacts for each category. Note: If authentication errors cause no measurable consequences for a category, there is "no" impact.

5.2 Determining Potential Impact of Authentication Errors

5.2.1 Potential Impact of Inconvenience, Distress, or Damage to Standing or Reputation:

- **Low—**at worst, limited, short-term inconvenience, distress or embarrassment to any party.
- **Moderate**—at worst, serious short term or limited long-term inconvenience, distress or damage to the standing or reputation of any party.
- **High**—severe or serious long-term inconvenience, distress or damage to the standing or reputation of any party (ordinarily reserved for situations with particularly severe effects or which affect many individuals).

5.2.2 Potential Impact of Financial Loss

- **Low**—at worst, an insignificant or inconsequential unrecoverable financial loss to any party, or at worst, an insignificant or inconsequential agency liability.
- **Moderate**—at worst, a serious unrecoverable financial loss to any party, or a serious agency liability.
- **High**—severe or catastrophic unrecoverable financial loss to any party; or severe or catastrophic agency liability.

5.2.3 Potential Impact of Harm to Agency Programs or Public Interests

- **Low**—at worst, a limited adverse effect on organizational operations or assets, or public interests. Examples of limited adverse effects are: (i) mission capability degradation to the extent and duration that the organization is able to perform its primary functions with noticeably reduced effectiveness, or (ii) minor damage to organizational assets or public interests.
- **Moderate**—at worst, a serious adverse effect on organizational operations or assets, or public interests. Examples of serious adverse effects are: (i) significant mission capability degradation to the extent and duration that the organization is able to perform its primary functions with significantly reduced effectiveness; or (ii) significant damage to organizational assets or public interests.
- **High**—a severe or catastrophic adverse effect on organizational operations or assets, or public interests. Examples of severe or catastrophic effects are: (i) severe mission capability degradation or loss of to the extent and duration that the organization is unable to perform one or more of its primary functions; or (ii) major damage to organizational assets or public interests.

5.2.4 Potential impact of Unauthorized Release of Sensitive Information

- **Low**—at worst, a limited release of personal, U.S. government sensitive or commercially sensitive information to unauthorized parties resulting in a loss of confidentiality with a low impact as defined in FIPS PUB 199.
- **Moderate**—at worst, a release of personal, U.S. government sensitive or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a moderate impact as defined in FIPS PUB 199.
- **High –** a release of personal, U.S. government sensitive or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a high impact as defined in FIPS PUB 199.

5.2.5 Potential impact to Personal Safety

- **Low**—at worst, minor injury not requiring medical treatment.
- **Moderate**—at worst, moderate risk of minor injury or limited risk of injury requiring medical treatment.
- **High**—a risk of serious injury or death.

5.2.6 Potential Impact of Civil or Criminal Violations

- **Low**—at worst, a risk of civil or criminal violations of a nature that would not ordinarily be subject to enforcement efforts.
- **Moderate**—at worst, a risk of civil or criminal violations that may be subject to enforcement efforts.
- **High**—a risk of civil or criminal violations that are of special importance to enforcement programs.

5.3 E-Authentication Analysis

Transaction 1: [Example] VPN/Keyfob access does not meet EAAL Level 4 (NIST 800-63) requirements.

Threat Vector	Likelihood	Impact	Risk	EAAL
Inconvenience, Distress, or Damage to Standing or Reputation				
Financial Loss				
Harm to Agency Programs or Public Interests				
Unauthorized Release of Sensitive Information				
Personal Safety				
Civil or Criminal Violations				
Overall Risk Level				

Transaction 2: [Example] Privileged-use access.

Threat Vector	Likelihood	Impact	Risk	EAAL
Inconvenience, Distress, or Damage to Standing or Reputation				
Financial Loss				
Harm to Agency Programs or Public Interests				
Unauthorized Release of Sensitive Information				
Personal Safety				
Civil or Criminal Violations				
Overall Risk Level				

6 RISK ASSESSMENT / EAAL RESULTS

Vulnerability 1: (Example – Terminated employees' userID's are not removed from the system)

Paired Threat(s)	Dependency Failures
Overall Risk Rating	Moderate

Recommended Safeguard: (Example - Remove employees' userID's from the system upon notification of termination.)

Vulnerability 2:

Paired Threat(s)	Dependency Failures
Overall Risk Rating	Moderate

Recommended Safeguard:

Vulnerability 2: VPN/Keyfob access does not meet EAAL Level 4 (NIST SP 800-63) requirements.

Paired Threat(s)	Inconvenience, Distress or Damage to Standing or Reputation
Overall Risk Rating	
Overall EAAL Rating	4

Recommended Safeguard: Migrate all remote authentication roles to CDC secure data network (SDN) or to another mechanism approved by the OCISO.

7 SUMMARY

The following table provides an overview of the vulnerabilities and recommended safeguards for **<System Name>.**

Table (?).<System Name> Risk Matrix

Vulnerability	Risk Level (High, Moderate, Low)	EAAL Transaction #	EAAL (1,2,3,4)	Recommended Safeguard
V-1..	Low	N/A	N/A	S-1.
V-2.	Moderate	2	2	S-2.

Implementing the recommended safeguards will reduce the overall risk exposure associated with the general vulnerabilities listed above to **Low**.

APPENDIX A ENTERPRISE THREAT STATEMENT

APPENDIX B NIST SP 800-53, REVISION 2, SECURITY BASELINE WORKSHEET

APPENDIX C RISK CALCULATION WORKSHEET

APPENDIX D RISK MITIGATION WORKSHEET

Controlled

Unclassified

Information

(CUI)

(When Filled IN)