

HEALTHY BODY WELLNESS CENTER, OFFICE OF GRANTS GIVEAWAY

---

**HEALTHY BODY WELLNESS CENTER  
OFFICE OF GRANTS GIVEAWAY  
SMALL HOSPITAL GRANTS TRACKING SYSTEM  
INITIAL RISK ASSESSMENT**

**PREPARED BY:**

**WE TEST EVERYTHING LLC**

**Jerry L. Davis, CISSP, Sr. Analyst**

<b>EXECUTIVE SUMMARY .....</b>	<b>4</b>
<b>1. INTRODUCTION.....</b>	<b>7</b>
Background.....	7
Purpose .....	7
Scope .....	7
Report Organization.....	8
<b>2. RISK ASSESSMENT APPROACH.....</b>	<b>9</b>
2.1 Step 1: Define System Boundary .....	9
2.2 Step 2: Gather Information .....	9
2.2.1 Interviews.....	10
2.2.2 Site Visit.....	10
2.2.3 Documentation.....	10
2.2.4 Network Scanning.....	10
2.3 Step 3: Conduct Risk Assessment .....	11
2.3.1 Impact.....	11
2.3.2 Likelihood .....	12
2.3.3 Risk .....	12
<b>3. SYSTEM CHARACTERIZATION .....</b>	<b>14</b>
System Overview.....	14
System Interfaces.....	14
Data .....	14
System and Data Criticality and Sensitivity .....	15
3.4.1 Criticality.....	15
3.4.2 Sensitivity.....	15
3.4.2.1 Confidentiality .....	15
3.4.2.2 Integrity .....	15
3.4.2.3 Availability.....	15
Users .....	16
<b>4. THREAT STATEMENT .....</b>	<b>17</b>
Threat Sources .....	17
Threat Actions .....	17
<b>5. FINDINGS .....</b>	<b>19</b>
Management Security .....	19
Operational Security .....	20

Technical Security .....	22
<b>APPENDIX A. RISK ASSESSMENT MATRIX.....</b>	<b>25</b>
<b>APPENDIX B. ACRONYMS.....</b>	<b>28</b>
<b>APPENDIX C. SAMPLE BASELINE SECURITY REQUIREMENTS .....</b>	<b>29</b>

## Executive Summary

The mission of the Healthy Body Wellness Center's (HBWC) Office of Grants Giveaway (OGG) is to promote improvements in the quality and usefulness of medical grants through federally supported research, evaluation, and sharing of information. The OGG distributes a variety of medical grants, but the majority of grants are disbursed to small hospitals. As a result, the OGG contracted We Automate Anything (WAA) to design and implement the Small Hospital Grant Tracking System (SHGTS).

The SHGTS is used to assist in the assignment and tracking of small hospital grants. The OGG assigns a particular grant to one hospital for one month and then the unused grant funds are rotated to another hospital for another month. The database tracks the initial delivery of the grant funds and its pertinent information, and then follows the grant through five hospital facilities. Only executive office staff can assign grant funds, but all grant users must complete their grant evaluations in the database. A weekly grant status report is prepared for the executive officer. Each month, the grant assignor is briefed on the grant status with reports generated from the database.

During the inception of the SHGTS, the Technical Review Board (TRB) and Configuration Control Review Board (CCRB) did not review the SHGTS because these boards did not yet exist. The SHGTS has never had a risk assessment or an OMB Circular No. A-130 review. As a result, the OGG contracted We Test Everything (WTE) to perform a risk assessment of the SHGTS.

To identify the potential threats and vulnerabilities associated with the SHGTS, WTE gathered information through the following techniques:

- Document review
- Onsite visits to the SHGTS computer room
- Interviews with designated OGG management and technical personnel
- Network scanning using an automated tool

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

- Management Security
- Operational Security
- Technical Security

A total of eight 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 the OGG 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 SHGTS 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 the OGG significantly. This exploitation would include the loss of some tangible assets or resources, which could impede the SHGTS 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 the OGG would be minor. This level of risk indicates that OGG management should be cautioned and corrective measures applied where required.

The findings section of this report analyzes each observation in detail. Appendix A summarizes the observations and presents the observation number and description as well as the potential threats, potential impacts, associated level, and countermeasures for each observation.

**Table ES-1**

<b>OBSERVATION NUMBER</b>	<b>OBSERVATION DESCRIPTION</b>	<b>RISK LEVEL</b>
<b>Management Security</b>		
M1	The accounts of SHGTS users who no longer require access may not be deleted immediately from the system.	<b>Medium</b>
<b>Operational Security</b>		
O1	A system security plan (SSP) has not been developed for the SHGTS.	<b>Medium</b>
O2	A disaster recovery plan (DRP) has not been developed for the SHGTS.	<b>Medium</b>
O3	There are no sign-in logs for visitors accessing the computer room.	<b>Low</b>
<b>Technical Security</b>		
T1	Passwords on the grants server are not required to be changed at least every ninety days.	<b>Medium</b>
T2	There is no limit to the number of invalid access attempts that may occur for a given user.	<b>Medium</b>
T3	Null session login may be possible.	<b>Low</b>

OBSERVATION NUMBER	OBSERVATION DESCRIPTION	RISK LEVEL
T4	Remote registry access is not restricted to administrators.	<b>High</b>

# **1. INTRODUCTION**

## **Background**

The mission of the Healthy Body Wellness Center's (HBWC) Office of Grants Giveaway (OGG) is to promote improvements in the quality and usefulness of hospital grants through federally supported research, evaluation, and sharing of information. The OGG distributes a variety of medical grants, but the majority of grants are disbursed to small hospitals. As a result, the OGG contracted We Automate Anything (WAA) to design and implement the Small Hospital Grant Tracking System (SHGTS).

The SHGTS is used to assist in the assignment and tracking of small hospital grants. The OGG assigns a particular grant to one hospital for one month and then the unused grant funds are rotated to another hospital for another month. The database tracks the initial delivery of the grant funds and its pertinent information, and then follows the grant through five hospital facilities. Only executive office staff can assign grant funds, but all grant users must complete their grant evaluations in the database. A weekly grant status report is prepared for the executive officer. Each month, the grant assignor is briefed on the grant status with reports generated from the database.

During the inception of the SHGTS, the Technical Review Board (TRB) and Configuration Control Review Board (CCRB) did not review the SHGTS because the boards did not exist. The SHGTS has never had a risk assessment or an OMB Circular No. A-130 review. As a result, the OGG contracted We Test Everything (WTE), under Contract No. ABCD12-34-E00567, Task Order # TO111111, to perform a risk assessment of the SHGTS.

## **Purpose**

The purpose of this report is to provide the HBWC and OGG management with an assessment of the adequacy of the management, technical, and operational security controls used to protect the confidentiality, integrity, availability, and accountability of the SHGTS. This risk assessment report identifies threats and vulnerabilities applicable to the SHGTS; 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 WTE performed during a two-and-a-half week period that will help OGG management understand the security posture of the SHGTS and its risk exposure. The risk assessment is part of the OGG's continuing effort to ensure compliance with federal policies and guidance as well as the HBWC's IT security policy.

## **Scope**

This risk assessment is limited to the SHGTS (a Microsoft Access 97 database), its host general support system (GSS) (JINX server EOC3FPR02\Groups\SSR), and the remote access server (RAS). The servers are housed in room 1234 at the HBWC's executive office facility. OGG staff

access the SHGTS from their workstations in room 5678. The risks were evaluated in the following security domains:

- Managerial
- Technical
- Operational

Site visits at HBWC headquarters were restricted to room 1234, where the JINX server and the RAS are located, and OGG 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.

## **Report Organization**

This document is divided into five sections. 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 WTE.
- Section 3 describes the characteristics of the SHGTS including the hardware, software, connectivity, data, and system users.
- Section 4 contains the threat statement including threat categories, threat agents, and actions.
- Section 5 provides an analysis of the findings in the management, technical, and operation security domains.

Additionally, the document contains three appendixes: Appendix A contains the Risk Assessment Matrix BLSR checklist, Appendix B lists acronyms and abbreviations listed throughout the report, and Appendix C provides the sample baseline security requirements (BLSR).



## 2. 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 WTE risk assessment methodology involved three major steps that are described below.

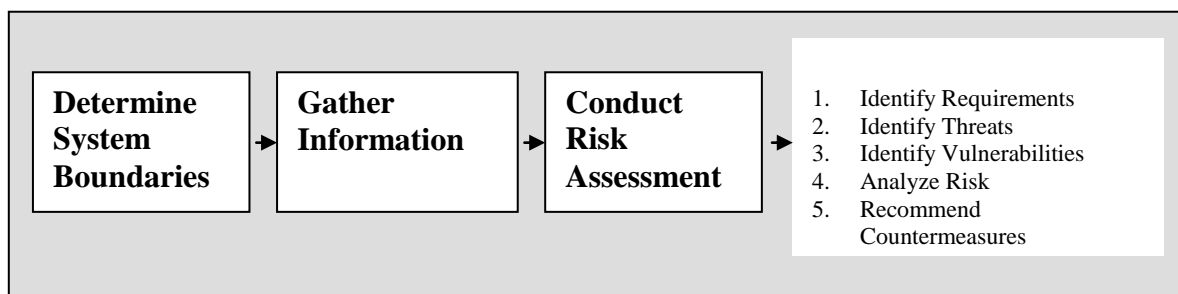
- Step 1 – Determine System Boundary
- Step 2 – Gather Information
- Step 3 – Conduct Risk Assessment.

The methodology used to perform the risk assessment for the SHGTS was developed by WTE with reference to the guidelines found in the following publications:

- *Federal Information Processing Standards (FIPS) Publication (PUB) 65: Guidelines for Automated Data Processing Risk Analysis*
- *National Institute of Standards and Technology (NIST) Special Publication 800-30: Risk Management Guide for Information Technology 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 as well as the impact (i.e., magnitude of loss) resulting from such exploitation.

**Figure 2-1: Risk Assessment Approach**



### 2.1 Step 1: Define System Boundary

The system boundaries, which determine the risk assessment scope, were restricted to the SHGTS and its Windows NT host JINX server EOC3FPR02\Groups\SSR. Meetings with the OGG system owner and the HBWC's information system security officer (ISSO) and chief information officer (CIO) along with reviewing the current system diagrams led to a determination of the boundaries.

### 2.2 Step 2: Gather Information

WTE assessed the SHGTS based on the risk assessment team's understanding of the operational environment and OGG and HBWC information technology (IT) policies and guidelines. Information about the SHGTS was gathered through interviews, site visits, documentation review, and the use of a network-scanning tool.

### **2.2.1 Interviews**

To collect relevant information, WTE developed a questionnaire on IT system management and operations of the SHGTS and support platform. The interviews were conducted on-site, via telephone, and through e-mail with the following OGG management and technical personnel:

- JINX server administrator
- OGG ISSO
- OGG CIO
- SHGTS Users

### **2.2.2 Site Visit**

The WTE team toured the computer room which houses the SHGTS hardware, software, and data at rooms 1234 and 5678 at executive office complex in the course of a day to observe the physical and environmental measures provided for the SHGTS. The visit also included a demonstration of how the system is accessed and administered, including adding and removing data. WTE also visited the homes of two OGG 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 the SHGTS. Listed below are all system and organizational documents reviewed in support of the assessment:

- OGG mission statement
- OGG organization chart
- SHGTS administrator's guide
- SHGTS user's guide
- SHGTS configuration management plan (CMP)
- OGG request for proposal (RFP) for development of tracking database
- WAA SHGTS documentation
- Standard operating procedures (SOPs).

### **2.2.4 Network Scanning**

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 JINX host was scanned once on two different days for a total of two scans.

## **2.3 Step 3: Conduct Risk Assessment**

The risk assessment encompassed the following subtasks:

- Determining the relative value of the SHGTS based on the criticality and sensitivity of the data the SHGTS processes, stores, and transmits
- Compiling the BLSR checklist
- Identifying and assessing potential threats
- Identifying and assessing potential vulnerabilities
- Determining risks
- Developing countermeasure recommendations.

The value of the SHGTS is measured in terms of system and data criticality and sensitivity, which are described in Section 3. The BLSR checklist encompasses the security requirements, policies, and guidelines applicable to the SHGTS. Appendix C provides a sample BLSR checklist.

To assess risks to the SHGTS, the WTE risk assessment team identified a list of potential threats that could exploit identified vulnerabilities of the SHGTS operational environment. Section 4 provides an analysis of the SHGTS threat environment.

Section 5 presents the findings and includes a discussion of the threat and vulnerability pair, identification of existing mitigating security controls, impact analysis discussion, risk rating, and recommended countermeasures. A summary of the findings is listed in Appendix B.

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 impact, likelihood, and an overall risk matrix.

### **2.3.1 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's sensitivity and its importance to the HBWC'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.

**Table 2.3.1–1: Impact Description**

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

### 2.3.2 Likelihood

Likelihood is determined by considering threats and vulnerabilities. The likelihood that a 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.

**Table 2.3.2–1: Likelihood Description**

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

### 2.3.3 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. 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.

**Table 2.3.3-1: Risk Rating**

	Likelihood		
Impact	High	Medium	Low
High	High	High	Medium
Medium	High	Medium	Low
Low	Medium	Low	Low

### 3. SYSTEM CHARACTERIZATION

#### System Overview

The SHGTS is a Microsoft Access 97 database that resides on the Windows NT application server JINX EOC3EOC3EOC3FPR02. The SHGTS application and its data are protected by the following built-in security mechanisms supported by the hardened Windows NT platform:

- Identification and authentication (I&A)
- Discretionary access control (DAC)
- Auditing

To segregate functions in support of SHGTS, three technical support personnel, who are members of the administrator group, have administrative rights to manage JINX EOC3EOC3EOC3FPR02. The SHGTS database administrator (DBA) does not have administrative privileges to the Windows NT operating system (OS).

The SHGTS database has been customized for group security to protect the application from design changes such as altering the visual basic for applications (VBA) code or modifying database objects. There are three categories of users for the SHGTS and they are described below.

- **Administrative:** Full control of the application including the ability to alter code and modify database objects
- **Executive:** Allows access to all reports and the ability to update key fields dealing with the assignment of grants
- **Basic:** Allows access to most, but not all forms, and the ability to update key fields relating to information about already assigned grants

A RAS (Windows NT) is in place for users that requires remote access to the SHGTS. Knowledge of the RAS phone number is limited to those users with a mission-essential need. Users access the RAS via dial-up networking or using a VPN solution.

#### System Interfaces

The SHGTS does not give or receive any data to or from any other major application (MA) or GSS. The SHGTS resides on JINX2 as its GSS, but otherwise does not interface with any other system. It is accessed from local OGG workstations. OGG staff may access this database when they connect remotely either through analog dialup to the RAS server or through the VPN connection.

#### Data

The SHGTS does not contain any privacy act information or proprietary data in its tables. Data stored in the SHGTS includes specific attributes about the grants such as distribution schedule, amount, control number, grant category, and sunset date. Information detailing grant distribution particulars including sponsoring staff, directing official, and date assigned, is also stored in the system.

## System and Data Criticality and Sensitivity

### 3.4.1 Criticality

The HBWC's *Information Systems Criticality Definition Process* defines automated information resources whose failure would not preclude the HBWC from accomplishing core business operations in the short to long term (a few hours to a few weeks) but would have an impact on the effectiveness or efficiency of day-to-day operations, as being mission supportive. The SHGTS does not contain any sensitive data and the failure of the SHGTS would not preclude the OGG from accomplishing core business operations in the short to long term (a few hours to a few weeks). However, failure of the system would have an impact on the effectiveness or efficiency of day-to-day operations. Consequently, the SHGTS 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 the SHGTS are described below.

#### 3.4.2.1 Confidentiality

**Low:** There is no privacy act or proprietary data to protect. No awardee information is tracked on the grants; the system only tracks grant specific data. If unauthorized personnel read data that they are not authorized to see, administrative action (such as grant suspension or a letter of reprimand) would be the most severe consequence. If competing grant candidates discovered the grant rating system, the financial impact would be under \$100,000.

#### 3.4.2.2 Integrity

**Medium:** The data maintained on the grant ratings does affect recommendations for particular grants. Since entire medical research establishments 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

**Low:** The reports are much easier to prepare with the database and it would be very inconvenient if the database were unavailable to quickly locate a specific grant. However, manual inspection of invoices (for receipt information) and office space (to locate grants) could be used. The consequences of the database being unavailable would probably never be even 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 following table summarizes the sensitivity levels. The overall system sensitivity level is determined by the highest value in the SHGTS level column. Therefore, the sensitivity level for the SHGTS is medium.

**Table 3.4.2.3-1: Sensitivity Rating**

<b>Sensitivity Class</b>	<b>SHGTS Level</b>
Confidentiality	Low
Integrity	Medium
Availability	Low

## **Users**

Only JINX2 users may gain access to the SHGTS since it is located on a JINX server. There is an additional logon unique to the database. There are three types of access allowed:

- Administrative, which provides total control
- Executive, which allows access to all reports and the ability to update key fields dealing with the disbursement of grants
- Basic, which allows access to most but not all forms, and the ability to update the fields relating to information about already disbursed grant funds



## 4. THREAT STATEMENT

### Threat Sources

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

**Table 4.1-1: Threat Sources**

Natural Disaster				
Storm damage (e.g., flood, rain, snow, tornado)	Fire	Lightning strikes		Earthquakes
Environmental Control Failures				
Long-term power failure	Chemicals	Pollution	Liquid leakage	Biological/chemical terrorism
Acts by Individuals				
Unauthorized network access	Arson		Blackmail	
Unauthorized disclosure	Browsing of privacy and proprietary information		Impersonation	
Unauthorized physical access	Distributed denial of service		Economic exploitation	
Theft	Fraud		Hacking	
Sabotage/vandalism/civil disorder	Interception		Labor dispute/strike	
Unauthorized action/alteration and sensitive information	Negligence/human error		Packet-sniffing	
Password-guessing (e.g., dictionary attack, brute force attack)	Malicious code		Data diddling	
Spoofing	System tampering		Falsified data input	
Unintentional data destruction	Virus implant		Web deface	

### Threat Actions

The OGG believes human threat agents or individuals—authorized and unauthorized—to be the biggest potential threats to the SHGTS system and its data. Humans could cause intentional or unintentional damage to the SHGTS that could impair the ability of the SHGTS to operate effectively. Possible human threat agents include the following:

- Insiders, disgruntled employees, dishonest employees, malicious persons

- Authorized users (e.g., privileged system users such as DBA, system administrator, and 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 grant disbursing organizations or foreign governments with an interest in the information held in the SHGTS
- Unauthorized users, who may use hacking or penetration techniques against the SHGTS system or JINX2 with the malicious intent of disrupting normal operations and causing harm to the SHGTS (e.g., computer criminals, terrorists, hackers, intruders, Internet users, perpetrators)

## 5. FINDINGS

This section presents the results of the risk assessment performed for the SHGTS application. An observation resulted when a vulnerability was identified with a threat that could exploit the vulnerability. BLSRs were developed to test general security requirements and system-unique security requirements. The BLSRs were derived from federal and HBWC policy, procedures and guidelines, and industry best practices. BLSRs and existing technical and procedural countermeasures that might mitigate the risks to the SHGTS environment were considered when assigning the risk level to each observation. The presentation of each observation consists of the following:

- Statement of the observation
- Description of the current environment in relation to the observation
- An assessment of the likelihood that a vulnerability will be exploited by a threat and the impact on the SHGTS of successful exploitation
- An assessment of the level of risk to SHGTS based on the threat and vulnerability assessment and any existing mitigating mechanisms or controls
- A recommendation of countermeasures that would reduce or eliminate the risk.

Risk levels are rated as *high*, *medium*, or *low*, as defined in Table 2.3.3-1. Related or similar observations are grouped together for discussion purposes.

During the risk assessment, a site visit to the SHGTS computer room located in room 1234 of executive office complex of the OGG facility in Washington, DC indicated that adequate environmental security was in place. The identified observations were grouped into the following three primary security areas, which are discussed in Sections 5.1–5.3:

- Management Security
- Operational Security
- Technical Security

### Management Security

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.

#### **Observation M1: The accounts of SHGTS users who no longer require access may not be deleted immediately from the system.**

Currently, the accounts of the users who no longer require access to the SHGTS application are not required to be deleted immediately.

- **Threat and Vulnerability Assessment:** Employees who no longer require access could disclose or alter SHGTS data (e.g., amount, recipient, and SSNs). The likelihood that the vulnerability would be exploited is estimated to be medium.

- **Potential Impact:** Exploitation of this vulnerability could result in input of falsified data, which could affect data integrity, which in turn could allow grants to not be properly assigned. The potential impact is medium.
- **Risk Estimation:** The likelihood of exploitation of this vulnerability is moderate and its potential impact is estimated as medium. Therefore, the risk is estimated as medium.
- **Recommendation:** Ensure that the ISSO receives communication from human resources when a user terminates employment. Require the site security officer (SSO) to deactivate and remove the SHGTS terminated user accounts from the system upon receipt of notification.

## Operational 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 three findings in the area of operational security.

### Observation O1: A system security plan (SSP) has not been developed for the SHGTS.

A review of all available documentation revealed that SHGTS does not have its own SSP. An SSP exists for the JINX GSS where the SHGTS resides, however, as an MA, the SHGTS is not covered under the JINX2 SSP.

- **Threat and Vulnerability Assessment:** Lack of documentation can lead to difficulty in supporting and enhancing the SHGTS in the future. The lack of complete documentation could also lead to incomplete security policy and procedure functionality being followed, thus leaving the system vulnerable to threats.
- **Potential Impact:** If security documentation is not available for access, users may involuntarily compromise the SHGTS by leaving it unsecured and susceptible to various vulnerabilities and threats, both internal and external. The impact of this vulnerability is medium.
- **Risk Estimation:** Based on the criticality of the SHGTS, the moderate likelihood of threat exploitation and moderate impact of such exploitation, the risk associated with this observation is estimated to be medium.
- **Recommendation:** In order to document the security processes of the system and to comply with the requirements of OMB Circular No. A-130, the OGG should develop an SSP for the SHGTS. At a minimum, the SSP should address the following:
  - Rules of the system
  - Training
  - Personnel controls
  - Incident response capability
  - Continuity of support
  - Technical security
  - System interconnection

OGG management should also refer to *National Institute of Standards and Technology (NIST) Special Publication 800-1: Guide for Developing Security Plans for Information Technology Systems* to assist them with the development of their SSP.

**Observation O2: A DRP has not been developed for the SHGTS.**

Backup capability is in place for the SHGTS via the JINX server. However, a DRP has not been developed and documented specifically for the SHGTS.

- **Threat and Vulnerability Assessment:** There is a reasonable probability that storms, lightning strikes, fire, long-term power failure, and threat actions by unauthorized persons (e.g., bomb threats) or authorized persons (e.g., inadvertent error) could destroy SHGTS hardware, software, and data, resulting in a denial of system availability. The overall likelihood of such an event is medium.
- **Potential Impact:** Without a documented and well-tested DRP, adequate controls might not be in place to mitigate a severe service interruption that might significantly affect the OGG's mission. Moreover, if controls are inadequate, even a minor interruption might result in lost or incorrectly processed data. If a hot site or a cold site has not been defined to ensure immediate service recovery and continuity of operations, a major system interruption requiring extensive recovery efforts would halt operations of the SHGTS. Depending on the level of disaster and the damage it caused, the potential impact of this threat could range from medium to high.
- **Risk Estimation:** Based on the criticality of the SHGTS, the moderate likelihood of threat exploitation, and the moderate impact of such exploitation, the risk associated with this observation is estimated to be medium.
- **Recommendation:** To comply with the requirements of OMB Circular No. A-130, the OGG should develop a DRP to ensure the ability to restore the SHGTS within a reasonable amount of time and to minimize the impact of a disaster. A DRP should include the following:
  - Identification of required support resources (e.g., deciding whether a hot site, a cold site, or a warm site should be used)
  - Documentation of detailed procedures for the transition to alternative backup resources during an emergency
  - Designation of DRP team members and definition of their roles and responsibilities
  - Coordination of efforts with the HBWC disaster network recovery procedures to minimize or eliminate conflicts
  - Development of procedures for restoring the system at an off-site location.

**Observation O3: There are no sign-in logs for visitors accessing the computer room.**

Visitors are required to wear visitor stickers when accessing the computer room, but the visitor stickers are not time-stamped and are available at the front door of the of the computer room without a guard's supervision. There was no sign-in log that documented visitors' access to the computer room.

- **Threat and Vulnerability Assessment:** Without sign-in logs for visitors accessing the computer room, the OGG may not adequately monitor visitors who enter and exit the computer room that houses the JINX servers. However, the likelihood of this vulnerability's being exploited is low since the computer room is staffed 24 hours a day and OGG personnel are trained to challenge visitors to the computer room.
- **Potential Impact:** Unauthorized persons or disgruntled employees could damage the server hardware, software, and data. Denial of server access could render the SHGTS application inaccessible to the users. The potential impact is estimated as medium.
- **Risk Estimation:** The estimated risk is low based on the likelihood of occurrence and the moderate impact.
- **Recommendation:** In order to minimize the vulnerabilities associated with this risk, the following items should be implemented:
  - Require visitors to sign an access log that details, at a minimum, their name, organization, purpose, and the date and time they enter and exit the computer room
  - Leave the temporary visitor stickers with the staff member responsible for computer room access so that the visitor stickers are controlled.

## Technical 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 four findings in the area of technical security.

**Observation T1: Passwords on the JINX server are not required to be changed at least every ninety days.**

**Observation T2: There is no limit to the number of invalid access attempts that may occur for a given user.**

These two observations were identified through interviews with the JINX Windows NT system administrator. Because these observations address similar issues, they are discussed together. Account policy of users directly affects the overall security of the computer system. Setting a minimum password and enabling account lockout are effective measures in preventing unauthorized people from accessing a system.

- **Threat and Vulnerability Assessment:** Unauthorized users who have valid user identifications (user IDs) may try and guess passwords in order to access the system. If they are able to access the system, their next step may be to elevate their privileges, which could affect the availability (denial of service) and/or integrity (manipulating data) of the system. Enabling account lockout and minimum password age are effective measures in deterring password guessing. The likelihood of threat exploitation is medium.
- **Potential Impact:** The direct impact of this vulnerability on the SHGTS is estimated to be medium because the entire Maryland medical community uses the OGG grants

recommendations. Data manipulated with malicious intent could cost the OGG between \$150,000 and \$300,000.

- **Risk Estimation:** Based on its medium likelihood and medium impact, the risk associated with this scenario is estimated to be medium.
- **Recommendation:** The Windows NT administrator should consult with OGG management to determine what the minimum password age and account lockout settings should be. The Windows NT administrator should then implement those changes on the system immediately.

#### **Observation T3: Null session login may be possible.**

This observation was identified by the network scan, which determined that the JINX server allowed remote computers to establish a null session.

- **Threat and Vulnerability Assessment:** For Windows NT networks with multiple domains, NT provides a mechanism for remote computers to establish an anonymous session without providing any credentials. This mechanism allows listing of users, groups, and share names on the remote computer in native Windows NT tools, such as the server manager, user manager, and access control list (ACL) editor. Allowing an attacker to obtain sensitive system information can help the attacker launch attacks against the JINX server. Although this is a known deficiency in the Windows NT operating system (OS) security and a number of hacker tools are freely available in the public domain that facilitate such exploitation, the OGG has firewalls and an intrusion detection system (IDS) in place. Therefore the likelihood of threat exploitation is low.
- **Potential Impact:** The direct impact of this vulnerability on the SHGTS is estimated to be low, but an attacker could use this information in planning and launching future attacks against the SHGTS. Unauthorized disclosure, alteration, and deletion of system and application data could adversely affect system integrity, confidentiality, and availability. The overall impact is medium.
- **Risk Estimation:** Based on its low likelihood and medium impact, the risk associated with this scenario is estimated to be low.
- **Recommendation:** Windows NT service pack (SP) 3 and later SPs provide a new pseudo group called Authenticated Users. This group is the same as the Everyone pseudo group except that Authenticated Users does not contain Anonymous. It is recommended that the Everyone group be replaced in all ACLs with the Authenticated Users group to disable nonessential services.

#### **Observation T4: Remote registry access is not restricted to administrators.**

This observation was identified by the network scan, which determined that the JINX server with IP address XXX.XXX.XXX.234 might allow unauthorized users to access the local registry from a remote computer.

- **Threat and Vulnerability Assessment:** The Windows NT registry is the repository for all system configurations, including security-related settings. By default, a Windows NT server allows only system administrators to access the system registry from a networked computer.

The remote registry access can be controlled by setting the permissions on the HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg so that only system and administrator accounts can access it. The network scan determined that either this key does not exist (which allows access to the Everyone group) or its permissions are set to allow some nonadministrators remote access to the registry.

In the past, Windows NT allowed anonymous access to the registry, a situation that was corrected with the introduction of SP 3. However, many freely available hacking tools still attempt to test this vulnerability. In addition, because null session log in may be possible (Observation T3), the likelihood of threat exploitation is high.

- **Potential Impact:** If this vulnerability were exploited, the JINX could be compromised. Because the configurations of Windows NT member servers mirror one another, compromising one server may allow the attacker to launch attacks against other connected servers. Therefore, the potential impact of this scenario is high.
- **Risk Estimation:** The likelihood and the adverse impact of exploitation are estimated as high. Therefore, the risk associated with this scenario is estimated to be high.
- **Recommendation:** The OGG should make mitigation of this vulnerability a top priority. The corrective measures are as follows:

Launch the Registry Editor (Reged32.exe) and navigate to the registry key, HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg. If the key does not exist, re-create it and set its permissions as follows:

- |                    |              |
|--------------------|--------------|
| – Administrator    | Full Control |
| – System           | Full Control |
| – Backup Operators | Read*        |

- \* If the backup operator role is separated from the administrator role, backup operators may need to have read access to this key.



## APPENDIX A.RISK ASSESSMENT MATRIX

No.	BLSR	Threats	Impact	Risk/Level	Priority	Countermeasure
Management Security						
M1	Accounts of SHGTS users who no longer require access are not deleted from the system immediately	Disgruntled employees, unauthorized users	Corrupted data, malicious code	Medium	6	<p>Require the supervisors of OGG terminated employees to inform the system responsible personnel (e.g., the OGG system manager) 5 days before the employment termination or, at the latest, immediately after the termination</p> <p>Require the system responsible persons to deactivate and remove the OGG terminated user accounts from the system upon notification of employment termination. Action should be taken immediately for privileged application users who are granted a user access code of 300 or above</p> <p>Require the system responsible personnel to review the list of application user accounts regularly to ensure that no inactive accounts exist on the SHGTS</p>
Operational Controls						
O1	A system security plan has not been developed for the SHGTS	Disgruntled employees, unauthorized users	Compromise of entire system	Medium	2	<p>Develop an SSP that, at minimum, addresses the following:</p> <ul style="list-style-type: none"> <li>• Rules of the system</li> <li>• Training</li> <li>• Personnel controls</li> <li>• Incident response capability</li> <li>• Continuity of support</li> <li>• Technical security</li> <li>• System interconnection</li> </ul>
O2	A continuity of operations plan (COOP) has not been developed for the SHGTS	Natural disaster, environmental control failures	Service interruption could significantly affect ability to perform work; loss of	Medium	3	In coordination with site facilities, develop and document a COOP to ensure system continuity during an emergency

No.	BLSR	Threats	Impact	Risk/Level	Priority	Countermeasure
			data			
O3	There are no sign-in logs for visitors accessing the computer room	Disgruntled employees, unauthorized users	Damage to SHGTS assets (hardware, software, data).	Low	8	Require visitors to sign an access log that details, at a minimum, their name, organization, purpose, and the date and time they enter and exit the computer room
Technical Security						
T1	Passwords not required to be changed at least every 90 days	Disgruntled employees, unauthorized users	Impersonation	Medium	4	Require that the minimum password age be set to 90 days or fewer.
T2	There is no limit to the number of invalid access attempts that may occur for a given use.	Disgruntled employees, unauthorized users	Password guessing (e.g. dictionary attack, brute force attack), denial of service, system compromise	Medium	5	Require that the account be locked out after three invalid login attempts
T3	Null session login may be possible	Disgruntled employees, unauthorized users	Information obtained could be used in planning and launching future attacks against the SHGTS  Unauthorized disclosure, alteration, and deletion of system and application data could adversely affect SHGTS integrity, confidentiality, and availability	Low	7	Create and set the following registry entry:  Run Registry Editor (Regedt32.exe) and select the following key in the registry:  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA  On the Edit menu, click Add Value and use the following entry:  Value Name: Restrict Anonymous Data Type: REG_DWORD Value: 1  (WARNING: Microsoft warns that using Registry Editor incorrectly can cause serious, system-wide problems that may require reinstallation of Windows NT for their correction.)

No.	BLSR	Threats	Impact	Risk/Level	Priority	Countermeasure						
T4	Remote registry access is not restricted to administrators	Disgruntled employees, unauthorized users, and hackers	<p>The JINX server could be compromised</p> <p>Compromising one server may allow the attacker to launch attacks against other connected servers</p>	High	1	<p>Launch the Registry Editor (Reged32.exe) and navigate to the Registry key, HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg. If the key does not exist, re-create it and set its permissions as follows:</p> <table><tr><td>Administrator</td><td>Full Control</td></tr><tr><td>System</td><td>Full Control</td></tr><tr><td>Backup Operators</td><td>Read*</td></tr></table> <p>* If the backup operator role is separated from the administrator role, backup operators may need to have read access to this key</p>	Administrator	Full Control	System	Full Control	Backup Operators	Read*
Administrator	Full Control											
System	Full Control											
Backup Operators	Read*											

## APPENDIX B.ACRONYMS

ACL	access control list
HBWC	Healthy Body Wellness Center
BLSR	baseline security requirement
C&A	certification and accreditation
COOP	continuity of operations plan
DAA	designated approving authority
DBA	database administrator
DRP	disaster recovery plan
FIPS	federal information processing standard
GSS	general support system
IDS	intrusion detection system
INFOSEC	information security
ISSO	information system security officer
IT	information technology
MA	major Application
NIST	National Institute of Standards and Technology
NT	new technology
OGG	Office of Grants Giveaway
OMB	Office of Management and Budget
OS	operating system
RAS	remote access server
RFP	request for proposal
SDLC	software development life cycle
SHGTS	Small Hospital Grants Tracking System
SOP	standard operating procedure
SP	Service Pack
SSO	system security officer
SSP	system security plan
VBA	visual basic for applications
VPN	virtual private network
WAA	We Automate Anything
WTE	We Test Everything

## APPENDIX C.SAMPLE BASELINE SECURITY REQUIREMENTS

No.	Security Requirement	Compliance			Comments
		Yes	No	Other	
MANAGEMENT CONTROLS					
Administration and Management Security					
Assignment of Responsibilities					
1.	Assign responsibility for security in writing to an individual trained in the technology used in the system and in providing security for such technology (OMB Circular No. A-130, Appendix III, Section B-a.1, b.1)				
2.	Assign responsibility for security in each system to an individual knowledgeable in the information technology used in the system and in providing security for such technology (OMB A-130, Appendix III, Section A-3, a.1)				
3.	Establish clear lines of authority and responsibility within the HBWC for the allocation of resources in securing critical infrastructure assets (Clinton)				
System/Application Security Plan					
4.	Require and develop system security plan (SSP) for all federal computer systems that contain sensitive information; update and review the SSP every three years (OMB A-130 Appendix III, Section A-3, a.2, b.2, Section B-a.2, b.2; Computer Security Act of 1987, Section 6.b)				
5.	The security plan is implemented and adequately secures the system or application (OMB A-130 Appendix III, Section A-3, a.2, b.2; A-130, 8a.2.c. (iv))				
Rules of Behavior					

No.	Security Requirement	Compliance			Comments
		Yes	No	Other	
6.	Establish rules of behavior for system and application use. The rules should clearly delineate responsibilities of and expectations for all individuals with access to the system (OMB A-130 Appendix III, Section A-3, a.2.a, b.2.a, Section B-a.2.a, b.2.a)				
<b>Training</b>					
7.	Provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or operation of a federal computer system within or under the supervision of the federal agency (OMB A-130 Appendix III, Section A-3, a.2.b, b.2.b, Section B-a.2.b, b.2.b; Computer Security Act of 1987, Section 5.a)				
8.	OPM regulation requires training for new employees within 60 days of hire (CIAO, 6)				
9.	Provide specialized training for all individuals given access to the system/application (OMB A-130 Appendix III, Section A-3, b.2.b, Section B, b.2.b)				
10.	The Office of the CIO and CIAO shall develop and promulgate training standards to ensure that personnel staffed in key positions within the HBWC's critical infrastructure are proficient in their jobs (Clinton)				
11.	Computer security training should be implemented into existing training programs such as orientation programs for new employees, and training courses involved with information technology systems equipment and software packages (NIST FIPS PUB 191, Appendix A GP9)				

No.	Security Requirement	Compliance			Comments
		Yes	No	Other	
12.	Training shall be provided to all users on the security features of the office automation software resident on their respective systems. They also need to understand the security features of the local area network (LAN) to which they are connected, as well as security issues related to the Internet, intranet, and/or extranet (CIAO, 6)				
13.	OPM regulation requires training when an employee enters a new position that deals with sensitive information (CIAO, p.6)				
14.	OPM regulation requires refresher courses based on the sensitivity of the information the employee handles (CIAO, 6)				
<b>Personnel Security</b>					
15.	Controls include individual accountability, least privilege, and separation of duties enforced by access controls (OMB A-130 Appendix III, Section A-3, a.2.c, b.2.c, Section B-a.2.c, b.2.c)				
16.	Segregation of duties within the IT function should include the following: separation between operations and programming, an independent control group, implementation of a librarian function, rotation of operators, closed-shop operations, and required vacations for all employees (OMB A-130; CIAO, 18)				
17.	Require personnel controls to screen individuals prior to being authorized for system access and periodic screening thereafter (OMB A-130 Appendix III, Section A-3, a.2.c, b.2.c)				
<b>Incident Response Capability</b>					

No.	Security Requirement	Compliance			Comments
		Yes	No	Other	
18.	Establish an incident response capability to provide help to users when a security incident occurs (OMB A-130 Appendix III, Section A-3, a.2.d Section B-a.2.d; CIAO, 47; Clinton)				
<b>Continuity of Support</b>					
19.	Establish continuity of support to periodically test the capability to provide continual service to users within a system (OMB A-130 Appendix III, Section A-3, a.2.e, Section B-a.2.e)				
20.	Areas of control will include continuity of service operations (CIAO, 18)				
21.	Establish contingency planning to periodically test the capability of the major application to perform and function in event of failure of its automated support (OMB A-130 Appendix III, Section A-3, b.2.d)				
<b>Information Sharing</b>					
22.	Limit the sharing of information that identifies individuals or contains proprietary information to that which is legally authorized, and impose appropriate conditions on use where a continuing obligation to ensure the confidentiality of the information exists (OMB A-130 A130-8.a.9.(c))				
23.	Assure that information which is shared with federal organizations, state and local governments, and the private sector is appropriately protected comparable to the protection provided when the information is within the application (OMB A-130 Appendix III, Section A-3, b.2.f, Section B-b.2.f)				
<b>Public Access Control</b>					



No.	Security Requirement	Compliance			Comments
		Yes	No	Other	
24.	Implement appropriate public access control where application promotes or permits public access. Additional security controls shall be added to protect the integrity of application and the confidence the public has in the application (OMB A-130 Appendix III, Section A-3, b.2.g, Section B-b.2.g)				
<b>Review of Security Controls</b>					
25.	Perform an independent review or audit of the security controls in each system or application at least every three years (OMB A-130 Appendix III, Section A-3, b.3, Section B-b.3)				
<b>Risk Assessment</b>					
26.	A risk analysis shall be performed whenever there is a significant change to the installation. A significant modification made to an SBU AIS or network shall require a review to determine the impact on the security of the processed SBU information (OMB A-130, III-4, 3.c.2.b)				
27.	Vulnerabilities assessments (reviews to identify existing weaknesses but not to determine if all requirements are met) of all assessable units (i.e., computer system or application) shall be performed, at a minimum, every three years (OMB Circular No. A-123, 6, 8c)				
28.	A vulnerability audit will be performed to find and document the vulnerabilities in critical information assets (CIAO, p.17)				
29.	Perform risk assessment to include a consideration of major factors in risk management to determine adequate security for the AIS (OMB A-130 Appendix III Section B)				

No.	Security Requirement	Compliance			Comments
		Yes	No	Other	
Authorize Processing					
30.	The system/application must be authorized prior to operation and reauthorized at least every three years thereafter (OMB A-130 Appendix III, Section A-3, a.4, b.4, Section B-a.4)				
Security Management					
31.	Standards should include minimum expected control guidance, including computer facilities controls, computer operations controls, input/output handling controls, network management controls, and technical support and user liaison policy (NIST SP 500-169)				
32.	Based on the results of the vulnerability assessments, remedial action plans will be developed to mitigate the impact of the threats identified (Clinton)				
33.	Implement and maintain IT programs to establish controls to assure adequate security for all information processed, transmitted, or stored in Federal AIS (OMB A-130 Appendix III, Section A-3)				
34.	Establish a level of security for all HBWC information systems that is commensurate with the sensitivity of the information and the risk and magnitude of loss or harm that could result from improper operation of the information system (OMB A-130, 8.1.g)				
Data and File Protection					
35.	Establish procedures to ensure the proper disposal of printed output based on the sensitivity of the data (Good business practices [GBP])				

No.	Security Requirement	Compliance			Comments
		Yes	No	Other	
36.	Establish procedures to ensure compliance with The Privacy Act (OMB A-130, 7.g)				
37.	Prohibit smoking and eating in magnetic computer tape storage libraries that contain permanent or unscheduled records (GBP)				
38.	The classification of sensitive data that requires protection shall be determined. Appropriate action will be taken to ensure that proper labeling banners are attached on the document (GBP)				
<b>Anti-Virus Protection</b>					
39.	LAN servers should be scanned by the area responsible for LAN management to assure no virus becomes resident on the LAN server (NIST FIPS PUB 191, Appendix A, 4.LA4)				
<b>Backup of Software and Data</b>					
40.	Backup procedures shall be properly documented, understood by IT personnel, and be integrated/coordinated with the organization's disaster recovery plan (GBP)				
41.	Backup procedures shall provide for off-site secured storage (GBP)				
42.	Off-site facilities should be sufficiently distant from the operating facility to provide adequate protection against major natural disasters (e.g., earthquakes and hurricanes) (GBP)				
43.	Weekly, monthly, and yearly backup of magnetic media is rotated and transported to an off-site storage facility (GBP)				

No.	Security Requirement	Compliance			Comments
		Yes	No	Other	
44.	External labels for diskettes or removable disks used when processing or temporarily storing permanent or unscheduled records shall include the following information: name of the organizational unit responsible for the records, descriptive title of the contents, dates of creation, data sensitivity, if applicable, and identification of the software and hardware used (GBP)				
<b>Configuration Management</b>					
45.	Systems should be thoroughly tested according to accepted standards and moved into a secure production environment through a controlled process (NIST SP 500-169)				
46.	Adequate documentation should be considered an integral part of the information system and be completed before the system can be considered ready for use (NIST SP 500-169)				
47.	All program changes should be approved before implementation to determine whether they have been authorized, tested, and documented (GBP)				
48.	Ensure that there is adequate and effective deployment of hardware or software/firmware changes across multiple sites (GBP)				
49.	Updates and changes in LAN communication hardware and software should be tested thoroughly to prevent unintentional access exposures (GBP)				
50.	Data standards are established and promulgated to ensure that consistent data definitions, coding schemes, naming conventions and formats are employed (GBP)				

No.	Security Requirement	Compliance			Comments
		Yes	No	Other	
51.	All operating systems and applications are patched with the latest vendor security patches as applicable (GBP)				
52.	A configuration management process is in place to test and install vendor security patches (GBP)				
53.	All applications are tested for input boundary conditions to prevent buffer overflows and other privileged access (GBP)				
54.	Passwords shall be encrypted (GBP)				
<b>TECHNICAL CONTROLS</b>					
<b>Communications Security</b>					
<b>Remote Access/ Dial-Up Access</b>					
55.	Appropriate access controls should be in place to support dial-up access to the organization's computer resources. Remote interfaces to the network should provide the same security available when connecting to the network locally (GBP)				
56.	Controls should be established to ensure that remote users are positively identified and authenticated before connection to the network is authorized (GBP)				
57.	Dial-up authority should only be granted to the organization's personnel who have a need to access the network (GBP)				
58.	Request for dial-up access must be approved by the requester's LAN administrator (GBP)				
59.	Procedure should be developed to facilitate the removal of dial-up capabilities when the organization's personnel are no longer authorized to dial-in (GBP)				
60.	Dial-up ports should be protected from unauthorized access (GBP)				

No.	Security Requirement	Compliance			Comments
		Yes	No	Other	
61.	Do not leave personal computers containing sensitive data which are connected to answering modems unattended (GBP)				
62.	If the auto-answer mode for a system is only used during normal working hours, disable that mode after hours (GBP)				
63.	Dial-up to the organization's computer resources must only occur through approved entry points (centrally managed) to ensure integrity of network security (GBP)				
<b>Firewalls</b>					
64.	Firewalls will be installed to control access to the internal network (CIAO, 33)				
65.	Firewalls will be used for blocking unauthorized incoming traffic (CIAO, 34)				
66.	<p>Intrusion detection systems (IDS) will be used to do the following:</p> <ul style="list-style-type: none"> <li>• Monitor and analyze user and system activity</li> <li>• Assess the integrity of critical system and data files</li> <li>• Recognize activity patterns involved in known attacks</li> <li>• Perform statistical analyses to spot abnormal activity patterns that may indicate an attack</li> <li>• Manage the operating system audit trail and alert system managers to user behavior</li> </ul> <p>(CIAO, 36)</p>				
67.	Vulnerability scanners will be used to identify weaknesses which could lead to security violations and uncover possible breaches (CIAO, 33)				

No.	Security Requirement	Compliance			Comments
		Yes	No	Other	
Encryption					
68.	Sensitive data files should be protected during transmission from one location to another (GBP)				
69.	Encryption should be available for sensitive information transmissions whenever needed (GBP)				
Interconnection					
70.	Require system interconnection to obtain written management authorization, prior to connecting with other systems (OMB A-130 Appendix III, Section A-3, a.2.g, Section B-a.2.g)				
71.	The area responsible for LAN management should secure the LAN environment within the site and interfaces to outside networks (NIST FIPS PUB 191, Appendix A, 3. NM3)				
Router					
72.	Screening routers shall have the capability to filter based on TCP and UDP ports as well as IP addresses and incoming network interfaces (GBP)				
73.	A screening router shall not be used as the sole segment of a firewall system; rather it should form a portion of the security bastion (GBP)				
74.	Inbound filtering will be performed to exclude or reject all data packets that have an internal host address (GBP)				
Inventory of Network Hardware and Software					
75.	Accurate records of hardware/software inventory, configurations, and locations should be maintained (NIST SP 500-169)				

No.	Security Requirement	Compliance			Comments
		Yes	No	Other	
76.	Develop and maintain a comprehensive inventory of IT equipment, hardware and software configurations, and major information systems/applications, identifying those systems/applications which process sensitive information (GBP)				
77.	An asset inventory shall be conducted to determine what systems, data, and associated assets (e.g., facilities, equipment, and personnel) constitute the critical information infrastructure (CIAO, 10)				
<b>Computer Security</b>					
78.	Interrelate technical, operational, and management controls to assure adequate security for all information processed, transmitted, or stored in federal AIS; (e.g., password protection will only be effective if both a strong technology is employed and it is managed to ensure that it is used correctly) (OMB A-130 Appendix III, Section B)				
79.	Establish technical controls to ensure appropriate security controls are specified, designed into, tested, and accepted in the application in accordance with NIST guidance (OMB A-130 Appendix III, Section A-3, b.2.e)				
80.	The area responsible for LAN management (or designated personnel) should rigorously apply available security mechanisms to enforce local security policies (NIST FIPS PUB 191, Appendix A, 3.NM1)				
<b>Identification and Authentication</b>					



No.	Security Requirement	Compliance			Comments
		Yes	No	Other	
81.	If automatic-login scripts for LAN or server access are utilized, the script cannot contain the password (GBP)				
82.	Users should be able to initiate a change of their password independently (GBP)				
83.	The system shall support a lock-out threshold if excessive invalid access attempts are input (GBP)				
84.	User IDs must be revoked if a password attempt threshold of three failed login attempts is exceeded (GBP)				
85.	All passwords that are included in a new system when it is delivered transferred or installed shall be immediately changed (FIPS 112, 3.4.2)				
86.	Passwords must be stored with one-way encryption (GBP)				
87.	No one but the user ID owner can have the ability to know or view passwords (GBP)				
88.	Users must be authenticated to the LAN before accessing LAN resources (NIST FIPS PUB 191, Appendix A, GP6)				
89.	LAN user IDs should not be permitted to initiate multiple concurrent logins to the LAN network (GBP)				
90.	Terminals, workstations, and networked personal computers should never be left unattended when user ID and password have been logged in (GBP)				
Access Control					

No.	Security Requirement	Compliance			Comments
		Yes	No	Other	
91.	Access control software and/or network operating system security should be kept current and controls limiting user access to sensitive data, applications, and programs should be in place (GBP)				
92.	Access controls should encompass systems and programs that edit, update, and store information. Controls should permit access only when specific authorization has been granted (GBP)				
93.	Users must be restricted to only those resources required for the efficient completion of their job responsibilities (GBP)				
94.	Where appropriate, terminals/ workstations should automatically log out if inactive for a specified period of time (GBP)				
<b>System Audit</b>					
95.	The system shall be able to create, maintain, and protect from modification, unauthorized access, or destruction an audit trail of accesses to the resources it protects (GBP)				
96.	For each recorded event, the audit record shall identify the following: date and time of the event, user, type of event, and the success or failure of the event (GBP)				
97.	The area responsible for LAN management should conduct timely audits of LAN server logs (NIST FIPS PUB 191, Appendix A, 3. NM6)				
98.	Unauthorized attempts to change, circumvent, or otherwise violate security features shall be detectable and reported within a known time by the system (GBP)				

No.	Security Requirement	Compliance			Comments
		Yes	No	Other	
99.	The security administrator will review reports to determine if there have been repeated unsuccessful attempts to log in to the network (GBP)				
<b>Object Reuse</b>					
100.	When a storage object (e.g., core area, disk file, etc.) is initially assigned, allocated, or reallocated to a system user, the system shall assure that it has been cleared (GBP)				
<b>OPERATIONAL CONTROLS</b>					
<b>Physical Security</b>					
101.	Employee access to the data site shall be controlled by an electronic access system (GBP)				
102.	Logs shall be required for recording all physical access to the facility by unauthorized individuals (GBP)				
103.	Escorts shall be provided for unauthorized individuals at all times. Escorts will have authorization for access to all areas of the facility (GBP)				
104.	The distribution of keys should be strictly limited and an effective control system established (GBP)				
105.	Tapes, disks, and other storage media shall be kept in a secure access-controlled environment when not being utilized by computer operations (GBP)				
106.	Secure methods are employed to safeguard PCs and related hardware that contain information during relocation (GBP)				
107.	File servers shall be located in areas where access is restricted (GBP)				

No.	Security Requirement	Compliance			Comments
		Yes	No	Other	
108.	The list of persons with authorized access should be reviewed and recertified annually (GBP)				
<b>Environmental Security</b>					
109.	The primary and backup processing sites as well as the tape storage areas shall be equipped with fire detection and suppression systems that detect and suppress fire in the incipient stage (GBP)				

## References

Clinton, Bill. (1998). Presidential decision directive /NSC 63. Retrieved from <http://www.fas.org/irp/offdocs/pdd/pdd-63.htm>

Computer security act of 1987: Public law 100-235 (H.R. 145) (1988). Retrieved from <http://epic.org/crypto/csa/csa.html>

Critical Infrastructure Assurance Office (CIAO). (2000). *Practices for securing critical information assets*. Retrieved from [http://www.infragard.net/library/pdfs/securing\\_critical\\_assets.pdf](http://www.infragard.net/library/pdfs/securing_critical_assets.pdf)

National Institute of Standards and Technology. (1994). *Guideline for the analysis of local area network security* (Federal information processing standards [FIPS] publication 191). Retrieved from <http://www.itl.nist.gov/fipspubs/fip191.htm>

National Institute of Standards and Technology. (1989). *Executive guide to the protection of information resources* (NIST SP 500-169).

Office of Management and Budget (OMB). OMB circular no. A-123. Retrieved from <http://www.whitehouse.gov/omb/rewrite/circulars/a123/a123.html>

Office of Management and Budget (OMB.) OMB circular no. A-130. Retrieved from [http://www.whitehouse.gov/omb/circulars\\_a130\\_a130trans4/](http://www.whitehouse.gov/omb/circulars_a130_a130trans4/)