Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

INFORMATION SECURITY WEAKNESSES POSE RISK TO OPERATIONS AND THE MISSION OF THE SUBSTANCE ABUSE AND MENTAL HEALTH SERVICES ADMINISTRATION

Inquiries about this report may be addressed to the Office of Public Affairs at Public.Affairs@oig.hhs.gov.

Thomas M. Salmon
Assistant Inspector General

September 2013
A-18-12-30420

Office of Inspector General

https://oig.hhs.gov

The mission of the Office of Inspector General (OIG), as mandated by Public Law 95-452, as amended, is to protect the integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of beneficiaries served by those programs. This statutory mission is carried out through a nationwide network of audits, investigations, and inspections conducted by the following operating components:

Office of Audit Services

The Office of Audit Services (OAS) provides auditing services for HHS, either by conducting audits with its own audit resources or by overseeing audit work done by others. Audits examine the performance of HHS programs and/or its grantees and contractors in carrying out their respective responsibilities and are intended to provide independent assessments of HHS programs and operations. These assessments help reduce waste, abuse, and mismanagement and promote economy and efficiency throughout HHS.

Office of Evaluation and Inspections

The Office of Evaluation and Inspections (OEI) conducts national evaluations to provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. These evaluations focus on preventing fraud, waste, or abuse and promoting economy, efficiency, and effectiveness of departmental programs. To promote impact, OEI reports also present practical recommendations for improving program operations.

Office of Investigations

The Office of Investigations (OI) conducts criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs, operations, and beneficiaries. With investigators working in all 50 States and the District of Columbia, OI utilizes its resources by actively coordinating with the Department of Justice and other Federal, State, and local law enforcement authorities. The investigative efforts of OI often lead to criminal convictions, administrative sanctions, and/or civil monetary penalties.

Office of Counsel to the Inspector General

The Office of Counsel to the Inspector General (OCIG) provides general legal services to OIG, rendering advice and opinions on HHS programs and operations and providing all legal support for OIG's internal operations. OCIG represents OIG in all civil and administrative fraud and abuse cases involving HHS programs, including False Claims Act, program exclusion, and civil monetary penalty cases. In connection with these cases, OCIG also negotiates and monitors corporate integrity agreements. OCIG renders advisory opinions, issues compliance program guidance, publishes fraud alerts, and provides other guidance to the health care industry concerning the anti-kickback statute and other OIG enforcement authorities.

Notices

THIS REPORT IS AVAILABLE TO THE PUBLIC
at http://oig.hhs.gov

Section 8L of the Inspector General Act, 5 U.S.C. App., requires that OIG post its publicly available reports on the OIG Web site.

OFFICE OF AUDIT SERVICES FINDINGS AND OPINIONS

The designation of financial or management practices as questionable, a recommendation for the disallowance of costs incurred or claimed, and any other conclusions and recommendations in this report represent the findings and opinions of OAS. Authorized officials of the HHS operating divisions will make final determination on these matters.

EXECUTIVE SUMMARY

Information security controls at the Substance Abuse and Mental Health Service Administration were inadequate because the Information Technology Infrastructure and Operations organization had not implemented and monitored the information security protections.

WHY WE DID THIS REVIEW

Office of Management and Budget Circular A-130, appendix III, requires that agencies implement and maintain a security program to assure that adequate security is provided for all support systems and major applications. The Federal Information Security Management Act of (FISMA) 2002 provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources and provides for development and maintenance of minimum controls required to protect Federal information and information systems.

The selection and implementation of appropriate security controls for an information system are important tasks that can have major implications on the operations and assets of an organization as well as the welfare of individuals and the Nation. Security controls are the management, operational, and technical safeguards or countermeasures employed within an organizational information system to protect the confidentiality, integrity, and availability of the system and its information.

OBJECTIVE

Our objective was to assess the adequacy of information security controls by evaluating Substance Abuse and Mental Health Services Administration's (SAMHSA) inventory management, patch management, antivirus management, event management, logical access, encryption, web vulnerability assessment and Universal Serial Bus (USB) port controls that are owned and managed by Information Technology Infrastructure and Operations (ITIO).

BACKGROUND

Office of Management and Budget Circular A-130, appendix III, requires that agencies implement and maintain a security program to assure that adequate security is provided for all support systems and major applications. FISMA provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources and provides for development and maintenance of minimum controls required to protect Federal information and information systems.

The selection and implementation of appropriate security controls for an information system are important tasks that can have major implications on the operations and assets of an organization as well as the welfare of individuals and the Nation. Security controls are the management, operational, and technical safeguards or countermeasures employed within an organization

information system to protect the confidentiality, integrity, and availability of the systems and its information.

HOW WE CONDUCTED THIS REVIEW

We reviewed selected information technology (IT) security controls in effect as of June 2012. These controls were inventory management, patch management, antivirus management, event management, logical access, encryption, web vulnerability management and USB port control management. For our review we used Federal and Departmental policies as our principle criteria. We did not review the overall internal control structure of SAMHSA. We performed our fieldwork at SAMHSA's offices in Rockville, Maryland.

WHAT WE FOUND

We found five categories of vulnerabilities:

1. Inventory Management. – The records given to us by ITIO had different totals of computers it managed for SAMHSA. Inventory was not tracked and managed effectively and therefore neither ITIO nor SAMHSA was able to account for all SAMHSA IT assets and ensure their security compliance.

2. Patch Management. – SAMHSA did not ensure that ITIO had effectively implemented its patch management program for those devices managed by ITIO. We identified vulnerabilities within the SAMHSA network that if exploited could have led to unauthorized disclosure, modification, or non-availability of critical data.

3. Antivirus Management. - ITIO and SAMHSA did not ensure that all of the SAMHSA computers and servers managed by ITIO had updated antivirus signatures.

4. Logical Access. – ITIO and SAMHSA did not implement an effective logical access control process for its user accounts and did not conduct sufficient reviews to ensure that only valid users had access to their information system.

5. USB Port Control Access. – ITIO and SAMHSA did not have any technical controls to prevent unauthorized and unencrypted USB devices from connecting to SAMHSA computers.

WHAT WE RECOMMEND

We recommend that SAMHSA meet with the Assistant Secretary for Administration to address the issues identified in this report. In addition, we recommend that SAMHSA ensure that ITIO implements the 17 detailed recommendations in Appendix A to address the specific findings we identified.

AUDITEE COMMENTS

In written comments on our draft report, SAMHSA concurred with all of our recommendations and described the actions they will take to implement them. We have included SAMHSA's comments in their entirety in Appendix D.

TABLE OF CONTENTS

INTRODUCTION

WHY WE DID THIS REVIEW

Office of Management and Budget Circular A-130, appendix III, requires that agencies implement and maintain a security program to assure that adequate security is provided for all support systems and major applications. The Federal Information Security Management Act (FISMA) provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources and provides for development and maintenance of minimum controls required to protect Federal information and information systems.

The selection and implementation of appropriate security controls for an information system are important tasks that can have major implications on the operations and assets of an organization as well as the welfare of individuals and the Nation. Security controls are the management, operational, and technical safeguards or countermeasures employed within the organizational information system to protect the confidentiality, integrity, and availability of the system and its information.

OBJECTIVE

Our objective was to assess the adequacy of information security controls by evaluating Substance Abuse and Mental Health Services Administration's (SAMHSA) inventory management, patch management, antivirus management, event management, logical access, encryption, web vulnerability assessment and Universal Serial Bus (USB) port controls that are owned and managed by Information Technology Infrastructure and Operations (ITIO).

BACKGROUND

Information Security

Office of Management and Budget Circular A-130, appendix III, requires that agencies implement and maintain a security program to assure that adequate security is provided for all support systems and major applications. FISMA provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources and provides for development and maintenance of minimum controls required to protect Federal information and information systems.

In recent years, legislation and Presidential Decision Directives have focused on safeguards for critical systems, assets, and infrastructures within the public and private sectors. The most recent enactment was FISMA, Public Law 107-347, Title III. The purpose of the law is to provide a comprehensive framework for ensuring the effectiveness of information resources that support Federal operations and assets, and provide a mechanism for improved oversight of Federal agency information security programs.

The selection and implementation of appropriate security controls for an information system are important tasks that can have major implications on the operations and assets of an organization

as well as the welfare of individuals and the Nation. Security controls are the management, operational, and technical safeguards or countermeasures employed within an organizational information system to protect the confidentiality, integrity, and availability of the system and its information.

Substance Abuse and Mental Health Services Administration's Mission

SAMHSA's mission is to reduce the impact of substance abuse and mental illness on America's communities. In 2011 alone, approximately 20 million people who needed substance abuse treatment did not receive it and an estimated 10.6 million adults reported an unmet need for mental health care. As a result the health and wellness of the individual is jeopardized and the unnecessary costs to society ripples across America's communities, schools, business, prisons & jails, and healthcare delivery systems.

SAMHSA's Division of Technology Management, Information Technology (DTM-IT) maintains and manages 24 laptops. The 24 laptops are used by SAMHSA's employees when on official travel. SAMHSA's, DTM-IT security management is responsible for patching and providing antivirus updates to the 24 laptops.

Office of the Secretary Managed Information Technology

The information technology (IT) needs of SAMHSA, are supported by a contractor. The contract is managed by the Office of the Secretary (OS) ITIO group. Through the ITIO, OS has awarded a competitive, multi-year IT service contract to Lockheed Martin. The Service Limitation Agreement (SLA) includes task order awards for computers and infrastructure support, for business application hosting, and for continuity of operations and disaster recovery planning. The contractor is responsible for managing the network infrastructure (i.e., the network, routers, firewalls, and general use servers) and user desktops for SAMHSA and other small OPDIVs. ITIO has oversight responsibilities over the contractor to ensure that all aspects of the contract are successfully completed.

ITIO is responsible for the core switches, routers, and firewalls used to connect to the SAMHSA network. ITIO is also responsible for antivirus and patching updates for workstations that SAMHSA's employees use.

HOW WE CONDUCTED THIS REVIEW

We reviewed selected SAMHSA IT security controls in effect as of June 2012. These controls were inventory management, patch management, antivirus management, event management, logical access, encryption, Web vulnerability assessment, and USB port control management. For our review we used Federal and Departmental policies as our principle criteria. We did not review the overall internal control structure of SAMHSA because it was not directly related to our objective. We performed our fieldwork at SAMHSA's offices in Rockville, Maryland.

FINDINGS

We conducted interviews with SAMHSA's and ITIO's security and IT personnel, reviewed policies and procedures, and tested controls in place. We found that some controls over the SAMHSA network and logical access were inadequate. We particularly noted that the ongoing problem with establishing an accurate computer inventory adversely affected the reliability of other processes such as patch and antivirus management.

Information security controls at SAMHSA were inadequate because ITIO had not implemented and monitored all the information security protections. Our report includes five findings relating to inventory management, patch management, antivirus management, logical access and Port Control Access for SAMHSA and ITIO senior management consideration.

Although we did not find evidence that these weaknesses had been exploited, exploitation could result in unauthorized access to, and disclosure of, sensitive information and disruption of critical operations for the SAMHSA. As a result, we believe the weaknesses are collectively and, in some cases, individually significant and could potentially compromise the integrity of the SAMHSA network.

Inventory Management

Inventory management is a critical process in effectively managing ITIO owned workstations, laptops, servers, and other IT components. ITIO must properly assess IT inventory to ensure accuracy and an adequate protection of all systems connected to the network. Additionally, the FISMA reporting template for FY 2012 requires that HHS, of which SAMHSA is a part, to fully account for and report all IT assets on its network (e.g., routers, servers, workstations, laptops, and blackberries) to provide visibility at the organization level.

Inventory was not tracked and managed effectively by ITIO and therefore neither SAMHSA nor ITIO were able to account for all of SAMHSA's IT assets. Our analysis identified the following exceptions:

- HHS departmental policy on the Property Management Information System (PMIS) which was mandated by the Assistant Secretary for Administration and Management (ASAM) on June 24, 2004, requires all assets be tracked in an asset inventory database. ITIO did not use PMIS to track Property Plant and Equipment (PP&E) records for those assets that were owned and managed by ITIO and used by SAMHSA's employees.

- ITIO had not established an effective method for IT asset inventory management. There were no controls in place to ensure an accurate count of those IT assets used by SAMHSA's personnel that were owned and managed by ITIO. During our review, SAMHSA and ITIO provided a number of inventory listings from these tools of total assets managed by ITIO that did not agree, revealing major discrepancies.

- SAMHSA's inventory list of servers showed four servers running Windows 2000 on its network, while the Symantec Risk Assessment Suite (RAS) tool managed by ITIO reported seven servers running Windows 2000.

- The report generated by the Altiris patch management tool did not display operating systems for two workstations. This was inconsistent with RAS, as RAS displayed 33 workstations running operating systems that were "unknown" under ITIO managed assets. Additionally, the RAS report also displayed 17 unauthorized SAMHSA managed machines active on the network.

- RAS displayed two Linux servers running on the SAMHSA network that, ITIO Security Operations Center staff could not identify.

Neither ITIO nor SAMHSA could explain why there was differences between the various listings nor why outdated operating system software remained in service. Without effectively controlling its hardware inventory, SAMHSA and ITIO were unable to account for and ensure security compliance of all its IT assets, such as current patch levels and anti-virus deployment status.

Because of these exceptions, SAMHSA and ITIO were unable to effectively implement standardized configuration requirements to protect SAMHSA's network from possible malicious attacks. Without an accurate accounting of its IT asset inventory, SAMHSA and ITIO were unable to know whether all computers were adequately protected. Using operating systems that are no longer supported by the vendor exposed SAMHSA computing resources and data owned and managed by ITIO to unnecessary risk because known security vulnerabilities were not remediated. All of these issues also contributed to SAMHSA's and ITIO's being unable to appropriately determine SAMHSA's overall security posture, and to effectively implement a security monitoring program that is both continuous and automated.

AUDITEE COMMENTS

SAMHSA concurred with all of our recommendations.

Patch Management

Patch management is the process of identifying, reporting, and effectively remediating information system flaws in an operational system. Timely patching helps organizations maintain operational efficiency and effectiveness, overcome security vulnerabilities, and maintain stability in the production environment. Organizations that cannot establish an information security control program that is both mature and based on a rigorous set of controls and processes might have a number of security vulnerabilities that, if exploited, could lead to unauthorized access of sensitive data. Minimizing this threat requires organizations to have properly configured systems, to use the latest software supported by the vendor, and to have the recommended efficiency and security patches installed.

ITIO did not effectively implement a patch management program for those assets it owns and manages for SAMHSA. ITIO gave us a partial listing of patches that it had implemented. We noted the following exceptions:

- ITIO was unable to provide patch status reports covering our requested timeframe (December – May 2012). Therefore, we were unable to determine whether servers and workstations owned and managed by ITIO for SAMHSA received the applicable security patches.

- ITIO could not provide us evidence to support that periodic reviews of installed and missing security patches were done on SAMHSA systems. We could not determine whether ITIO had given patch implementation reports to SAMHSA's Chief Information Security Officer (CISO).

- Neither SAMHSA nor ITIO were reconciling inventory reports with patching or antivirus compliance reports. We found inconsistencies within the inventory reports provided by ITIO. As a result, we were unable to determine whether all workstations and servers were properly patched. For example, an ITIO inventory listing displayed 748 workstations but the patch compliance report displayed 707 machines.

- SAMHSA officials stated that non-governmental machines were allowed to access SAMHSA's network.

In addition, we identified four Windows 2000 Servers and one Windows Server 2003 R2 SP1 on the ITIO inventory listing. Windows 2000 Server reached its end of life (EOL) on July 13, 2010. Windows Server 2003 R2 SP1 reached its EOL on March 13, 2009. In the patching and antivirus world, end of life indicates that the computer product has reached its useful lifetime and the vendor will no longer be marketing, selling, supporting or provide patches.

SAMHSA relied on ITIO to generate periodic reviews and reports for SAMHSA's IT management. However, ITIO failed to provide that information to us. Additionally, neither SAMHSA nor ITIO reconciled the inventory to validate the accuracy of the assets owned and managed by ITIO for SAMHSA.

For non-government machines, SAMHSA stated that it follows the HHS/ITSC Program Security Guide. This guideline requires that foreign hardware (non-governmental machines), whether laptops or desktops, be configured with a minimum baseline security set-up. The baseline included patching, antivirus, file encryption, and firewall settings. Systems that were not configured to meet these requirements were required to be issued a network connection denial notice.

Without proper procedures for patch installations and monitoring, SAMHSA and ITIO exposed its operating systems to attacks. Running un-patched computers and servers left SAMHSA systems susceptible to exploits that could have led to unauthorized disclosure, modification, or non-availability of critical data. Compromised computers can be used as a jumping off point for hackers to attack other resources in the network. Furthermore, as part of an effective information

security continuous monitoring strategy, the SAMHSA CISO should have received monthly reports for controls with more volatility (e.g., patch and anti-virus distribution) or on controls for which there have been weaknesses or lack of compliance.

In addition, without an accurate inventory of components within the organization, SAMHSA and ITIO were unable to ensure that all applicable computers and servers were properly patched.

AUDITEE COMMENTS

SAMHSA concurred with all of our recommendations.

Antivirus Management

Antivirus management is the automated process used to effectively identify, isolate, and eliminate suspected malicious software for computer security virus protection. Antivirus software should be implemented and maintained at critical information system entry points and computers on a network to detect and eradicate malicious code transported by email, removable media, or other methods. Antivirus controls are important for the detection and removal of malicious software such as computer viruses, worms, and trojans, which can infect a computer system or network.

Our analysis of the antivirus management reports indicated that not all ITIO owned and managed computers and servers used for SAMHSA's operations had updated signatures. An antivirus signature is an algorithm or hash (a number derived from a string of text) that uniquely identifies a specific virus.

Neither SAMHSA nor ITIO security management gave any indication as to why there was no documented evidence of antivirus alert remediation. In addition, SAMHSA and ITIO management did not include a follow-up process for computers with outdated timestamps or process for servers within ITIOs antivirus Standard Operating Procedures (SOP). We noted the following exceptions from the antivirus data and reports provided:

- We judgmentally selected thirty desktop and laptop user accounts from SAMHSA's Active Directory (AD) list to review the antivirus engine and signature timestamps. We reviewed SAMHSA's Symantec Endpoint Protection report dated August 09, 2012. The report indicated that virus signatures for:

    - Two of the thirty ITIO owned and managed systems were last updated with the antivirus signature 47 and 364 days prior, to report date.

    - One ITIO owned and managed server was last updated with the antivirus signature on November 21, 2011.

- We were unable to determine whether all servers were updated with applicable antivirus timestamps due to SAMHSA's and ITIO's inability to reconcile the various server inventory lists.

- Three servers that received the latest Symantec Signature updates for antivirus were not included on one of the ITIO inventory server lists.

- There were 16 servers not found on the Symantec Signature Timestamp antivirus listing that appeared on the two server listings provided by ITIO. Therefore the status of these servers could not be determined.

- Both SAMHSA and ITIO were alerted 120 times from ITIO's Nitro Security Information and Event Management (SIEM) tool, between 04/14/2012 to 08/27/2012. However, neither SAMHSA nor ITIO was able to provide documentation to support follow-up or remediation of the alerts.

- ITIO antivirus SOP did not contain follow-up processes for machines not in compliance with latest antivirus time stamp and did not cover follow-up procedures for servers.

- The ITIO's computer naming convention did not identify SAMHSA or any of the other OPDivs, nor reference either the state or district (e.g. MD or Washington, DC) associated with the IP address. HHS policy requires that the inventory database should at a minimum distinguish the name, location, asset identification (ID), owner, and description of the use.

Neither SAMHSA nor ITIO security management could provide a reason why the timestamps for the two tested computers were not current. ITIO management did not create specific naming conventions for its laptops/desktops and/or servers to differentiate computer inventory between the OPDIVs.

Without adequately documented procedures, SAMHSA computing resources that are owned and managed by ITIO may not be effectively protected.

Viruses can cause serious damage to systems. Failure to keep antivirus software signatures up to date can result in the widespread distribution of viruses within SAMHSA's network. The concerns relating to antivirus are that:

- Without proper installation of antivirus software, users may mistakenly believe that their system are virus-free and may inadvertently spread a virus.

- Without proper naming conventions, ITIO cannot achieve effective accountability for updating antivirus.

- Without indicating actions taken, no determination can be made that security management has reviewed and/or remediated the virus alert.

AUDITEE COMMENTS

SAMHSA concurred with all of our recommendations.

Logical Access

Logical access controls provide reasonable assurance that management protects computer resources against unauthorized modification, disclosure, loss, or impairment. Inadequate access controls over computerized data increases the risk of destruction or inappropriate disclosure of data. Logical access controls include the process over authorization requests, creation of accounts, certification/approval of access, and termination processes.

We reviewed user account privileges in AD, performed an assessment of key AD dates, and reviewed Virtual Private Network (VPN) data. Our analysis identified the following exceptions to the 644 SAMHSA user accounts:

- ITIO had 15 SAMHSA user accounts with a last password change date greater than 60 days.

- ITIO had seven SAMHSA user accounts with a last log on date greater than 60 days.

- ITIO had one SAMHSA account with a password status of "Not Required".

- ITIO had three SAMHSA remote user accounts with last password change date greater than 60 days.

- ITIO had one SAMHSA remote user account with last log on date greater than 60 days.

- ITIO had four separated SAMHSA employees that were still on the AD listing that had not been disabled. One terminated employee was also on the remote user list.

- ITIO had several SAMHSA generic and generic administrative user accounts still in their Active Directory.

SAMHSA's and ITIO's security management stated that they did not review the user access privileges for SAMHSA's AD and remote access accounts.

Inadequate controls over access accounts diminishes the safety and reliability of data, and increases the risk of an unauthorized user gaining access, or an authorized user elevating his or her privileges without management knowledge. Without a logical control process that meets requirements, management is not assured that individual users are properly identified, access is restricted to properly authorized users, and user activity is restricted to authorized functions.

AUDITEE COMMENTS

SAMHSA concurred with all of our recommendations.

USB Port Control Access

In today's computing environment, the confidentiality of information stored on USB devices faces many threats, both unintentional (e.g., human error, device loss) and intentional (e.g., theft). Intentional threats are posed by people with many different motivations, including the desire to cause mischief and disruption and to commit identity theft and other fraud. Someone with physical access to a device has many options for attempting to view or copy the information stored on the device. Malware, another common threat, can give attackers unauthorized access to a device, transfer information from the device to an attacker's system, and perform other actions that jeopardize the confidentiality of the device's information.

To prevent unauthorized access to information, particularly to personally identifiable information (PII) and other sensitive data, the information needs to be secured. Encryption is the primary security control for restricting access to sensitive information stored on end-user devices. Encryption may be applied granularly to individual files or broadly to all stored data. The appropriate encryption solution depends primarily on the type of storage, the amount of information that needs to be protected, where the storage will be located, and the threats that need to be mitigated. Encryption should always be used on portable devices that are used to store or transport sensitive information.

ITIO security management did not have technical controls on the computers they owned and managed for SAMHSA to prevent unauthorized and unencrypted USB devices from connecting to SAMHSA computers. The security software used allowed users to choose between encrypting and not encrypting the devices. However, we found that if the user elects not to encrypt, the software still allowed the user to download data onto the device.

We judgmentally selected 10 computers, and used an application called USBDeview to list all USB devices that had been connected to the computers. The USBDeview software detected multiple unencrypted Pantech phones, android phones, wireless Bluetooths and USB mass storage devices that had been connected to the 10 computers tested. SAMHSA used the Checkpoint Endpoint Security Tool which could provide device control on the ten computers tested. However, based on the results of our testing of devices that had been attached to SAMHSA's computers through USB ports SAMHSA did not use these functions to block unauthorized devices from attaching to their computers and preventing data from being written onto unauthorized USB devices. Without such controls, there is a risk that confidential data could be written onto an unauthorized/unencrypted USB device and taken out of the SAMHSA's spaces, possibly resulting in a data breach.

ITIO did not use the full functionality of its Checkpoint Endpoint Security Tool to block unauthorized devices from attaching to the computers ITIO owned and managed for SAMHSA.

Without sufficient USB controls, there is a risk that malicious software could be transferred from the USB devices to those computers owned and managed by ITIO for SAMHSA and subsequently into the SAMHSA's network. In addition, critical/sensitive information could be stored and transferred to unencrypted devices and removed from SAMHSA work spaces.

AUDITEE COMMENTS

SAMHSA concurred with all of our recommendations.

RECOMMENDATIONS

We recommend that SAMHSA meet with the Assistant Secretary for Administration to address the issues identified in this report. In addition, we recommend that SAMHSA ensures that ITIO implements the 17 detailed recommendations in Appendix A to address the specific findings we identified.

APPENDIX A: RECOMMENDATIONS

Findings	Risk	Office of Inspector General Recommendations
To address the Inventory Management issues identified in this report, we recommend that SAMHSA ensures ITIO:	**High**	• Implements the Departmental Property Management Information System (PMIS) in order to provide a continuous monitoring program to SAMHSA that will accurately account for all IT assets, and provide comprehensive reporting to the SAMHSA Chief Information Officer (CIO). • Updates inventory to include all computers and servers connecting to the SAMHSA network that are managed by ITIO. Employ controls that ensure an effective method for tracking computer inventory is implemented. • Upgrades or replace all servers with End-of-Life (EOL) operating systems to operating systems supported by the vendor
To address the Patch Management issues identified in this report we recommend that SAMHSA ensures ITIO:	**High**	• Security team ensure that patch reports are accessible to SAMHSA's Chief Information Security Officer. • Should reconcile SAMHSA's inventory and patch report data, at least monthly, to determine whether all assets are appropriately patched.
To address the Antivirus Management issues identified in this report we recommend that SAMHSA ensures ITIO:	**High**	• Update all computers and servers running out of date antivirus timestamp signatures. • Establish effective procedures to monitor and remediate computers with out-of-date timestamp signatures. • Document logging alerts that have been remediated. • Add the following processes to ITIO's Infrastructure Operations Standard

		Operating Procedure (SOP): – Follow-Up process for computers not in compliance with latest antivirus time stamps within SOP. – Process for server antivirus management. • Create naming conventions that include computer names that will define which organization it has been assigned to.
To address the Logical Access issues identified in this report we recommend that SAMHSA ensures ITIO:	**High**	• Disable accounts inactive greater than 60 days and subsequently delete accounts determined to be no longer needed greater than 90 days. • Delete user accounts of terminated employees. • Should disable, delete, or provide a waiver for the user account with a password status of "Not Required" • Periodically review access user control lists to determine if accounts are still needed.
To address the USB Port Control Access issues identified in this report we recommend that SAMHSA ensures ITIO:	**High**	• Restrict personnel from connecting unauthorized USB devices to computers. • Prevent sensitive data from being written to unauthorized/unencrypted USB devices. • Enforce the Department information security policy that restricts the connection of personally owned equipment to Department systems or networks.

APPENDIX B: AUDIT SCOPE AND METHODOLOGY

SCOPE

We reviewed selected IT security controls in effect as of June 2012. These controls were inventory management, patch management, antivirus, event management, logical access, encryption, web vulnerability assessment and Universal Serial Bus (USB) port control management. Network management refers to the activities that pertain to the operations, administration, maintenance, and configuration of networked systems. Areas of network management included in this audit were limited to patch management, antivirus management and event management. We did not review the overall internal control structure of SAMHSA. We performed our fieldwork at SAMHSA's offices in Rockville, Maryland.

METHODOLOGY

We audited SAMHSA's information security controls by reviewing policies and procedures, interviewing employees, reviewing and analyzing records and reviewing documentation. We reviewed:

- Inventory management process for IT assets to ensure that management monitors and protects property and other assets against waste, loss, unauthorized use, or misappropriation
- Patch management procedures for patch installations and monitoring
- Antivirus versions, scan engines and signature timestamps
- Logical access process, we performed an analysis of their ITIO managed Active Directory (AD) and remote user Virtual Private Network (VPN) accounts and
- Port control access that prevents unauthorized access to information, particularly to personally identifiable information (PII) and other sensitive data

For the principle criteria used for this review see Appendix C.

APPENDIX C: CRITERIA AND FEDERAL REQUIREMENTS

Inventory Management

NIST SP 800-53, Page F-44, Revision 3, Information Security, dated August 2009, CM-8 Information System Component Inventory – The organization develops, documents, and maintains an inventory of information system components that: Accurately reflects the current information system; Is consistent with the authorization boundary of the information system; Is at the level of granularity deemed necessary for tracking and reporting; and is available for review and audit by designated organizational officials. This includes the following control enhancements:

1. The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.
2. The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

NIST SP 800-53 Rev 3, section CM-8; page F-44 – Information System Component Inventory:

> "Supplemental Guidance: Information deemed to be necessary by the organization to achieve effective property accountability can include, for example, hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a networked component/device, the machine name and network address."

HHS-OCIO Policy for Information Systems Security and Privacy Handbook, Section 1.8, P-AM.2 and P-AM.3, page 11, states all assets shall be tracked in an asset inventory database to include (at a minimum) name, location, asset identification (ID), owner, and description of use. Section 1.8 further states that OPDIVs: Develop and conduct procedures for verifying accuracy for OPDIV or STAFFDIV IT asset inventories. Collaborate with Designated Approving Authorities (DAAs)/Authorizing Officials (AOs), Information System Security Officers (ISSOs), field technicians, and others as necessary to conduct verification procedures. Engage/use the HHS Property Management Information System, as appropriate.

HHS-OCIO Policy for Information Systems Security and Privacy Handbook, Section 2.8, Remote Access S-RMT.1, page 42, states – All computers and devices, whether government-furnished equipment (GFE) or contractor-furnished equipment (CFE), that require any network access to a Department or OPDIV network or system shall be securely configured and meet at least the following security requirements: (i) up-to-date system patches, and (ii) current anti-virus software; and (iii) functionality that provides the capability for automatic execution of code disabled.

HHS Logistics Management Manual (LMM) Policy and Procedures, Executive Summary section page iii and page 3, states that the "management of property and other programs and activities"; to include ordering, receiving, storing, distributing, accounting for, maintaining, and

disposing of supplies and equipment. This includes the Departmental Property Management Information System (PMIS), which is used to track Property Plant and Equipment (PP&E) records. PMIS provides reasonable assurances that funds, property, and other assets are protected against waste, loss, unauthorized use, or misappropriation. The PMIS is the enterprise-wide PP&E management system as mandated by ASAM on June 24, 2004. Furthermore, in section 1.1.8 of the manual it also states that HHS logistics OPDIVs and STAFFDIVs shall use the Department's PMIS as the PP&E System of Record. All other legacy systems are not the System of Record, and shall be decommissioned.

Patch Management

NIST SP 800-40, Version 2, Creating a Patch and Vulnerability Management Program, page ES-1 and page 2-2, par 8, executive summary states that timely patching is critical to maintain the operational availability, confidentiality, and integrity of IT systems. It also states that a central patch and vulnerability group (PVG) should deploy patches automatically to IT devices using enterprise patch management tools. Automated patching tools allow an administrator to update hundreds or even thousands of systems from a single console.

NIST SP 800-53, Page F-44, Revision 3, Information Security, dated August 2009, CM-8 Information System Component Inventory – The organization develops, documents, and maintains an inventory of information system components that: Accurately reflects the current information system; Is consistent with the authorization boundary of the information system; Is at the level of granularity deemed necessary for tracking and reporting; and is available for review and audit by designated organizational officials. This includes the following control enhancements:

1. The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.
2. The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

NIST SP 800-53 Rev 3, section CM-8; page F-44 – Information System Component Inventory:

> "Supplemental Guidance: Information deemed to be necessary by the organization to achieve effective property accountability can include, for example, hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a networked component/device, the machine name and network address."

NIST SP 800-137, section 3.4.2, page 32, states "Organizations define security status reporting requirements in the ISCM strategy. This includes the specific staff/roles to receive ISCM reports, the content and format of the reports, the frequency of reports, and any tools to be used." It continues: "Organizations may consider more frequent reports for specific controls with more volatility or on controls for which there have been weaknesses or lack of compliance."

HHS-OCIO Policy for Information Systems Security and Privacy Handbook, Section 2.10 Personally-Owned Equipment and Software (POES) states:
S-POES.1, page 44 – Prohibit connection of personally-owned equipment to Department systems or networks without written authorization from the appropriate OPDIV CIO or his/her designated representative.
S-POES.1.1, page 44 – Scan personally-owned equipment that has received the proper written authorization to ensure it complies with OPDIV/STAFFDIV system requirements (e.g., updated patches) before connecting it to Department systems or networks. Note: Use of personally-owned equipment or CFE on government networks is recognized as potentially introducing a high level of risk to the government computing infrastructure. These connections shall only be permitted as a risk-based decision made by the OPDIV CIO or his/her designated representative.
S-POES.4, page 44 – Prohibit personally-owned or non-Department equipment from processing, accessing, or storing PII unless approved in writing by the OPDIV SOP.

HHS-OCIO Policy for Information Systems Security and Privacy Handbook, Section 2.8, Remote Access S-RMT.1, page 42, states – All computers and devices, whether government-furnished equipment (GFE) or contractor-furnished equipment (CFE), that require any network access to a Department or OPDIV network or system shall be securely configured and meet at least the following security requirements: (i) up-to-date system patches, and (ii) current anti-virus software; and (iii) functionality that provides the capability for automatic execution of code disabled.

Antivirus Management

NIST 800-42, page 3-9, section 3.7, Virus Detectors; paragraph 6; states that the most important aspect of virus detection software is frequent, regular updates of virus definition files and on-demand updates when a major virus is known to be spreading throughout the Internet. When the database is updated frequently, the anti-virus software will detect more viruses. If these preliminary steps are taken, the chances of a major virus infection are minimized.

HHS OCIO Handbook, Section 1.6 P-CM.14, page 9 – Ensure current anti-virus software is included, as appropriate, on systems connected to the HHS network, and that the software is configured to automatically perform periodic virus scanning.

HHS-ITIO Standard Operating Procedures for Anti-Virus Management, page 4 - provides the process to be followed for performing daily antivirus management for all users with access to the Check Point Endpoint Security console.

HHS-PSC-ITIO Foreign Hardware Scanning Guide, page 3 "Executive Summary", states – "HHS/ITSC Program Security Guide requires that foreign hardware whether laptops or desktops to be configured with a minimum baseline security posture to include:

1. "Employ industry recognized antivirus software with current signature files"

Logical Access

NIST SP 800-12, section 10.2, page 112, states that effective administration of users' computer access is essential to maintaining system security.

NIST SP 800-14, section 3.5.2, page 28, generally states that organizations should have a process for (1) requesting, establishing, issuing, and closing user accounts; (2) tracking users and their respective access authorizations; and (3) managing these functions.

NIST SP 800-53 Rev 3, section AC-2; page F-4 – Account Management:

> "Supplemental Guidance: The identification of authorized users of the information system and the specification of access privileges is consistent with the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by organizational officials responsible for approving such accounts and privileged access."

HHS-OCIO Policy for Information Systems Security and Privacy Handbook, Section 2.8, Remote Access S-RMT.1, page 42, states – All computers and devices, whether government-furnished equipment (GFE) or contractor-furnished equipment (CFE), that require any network access to a Department or OPDIV network or system shall be securely configured and meet at least the following security requirements: (i) up-to-date system patches, and (ii) current anti-virus software; and (iii) functionality that provides the capability for automatic execution of code disabled.

HHS-OCIO Policy for Information Systems Security and Privacy Handbook, page 49 Section 2: HHS Assignments and Selections in accordance with NIST SP 800-53 Rev. 3 states:

> "The information system automatically disables inactive accounts after…60 days or less."

HHS-OCIO Policy for Information Systems Security and Privacy Handbook, page 40 Section 1: Department-wide Program-level and System-level Controls; subsection 2.5 Passwords; paragraph states:

> "S-PSWD.3 – Ensure passwords are changed at least every 60 days, immediately in the event of known or suspected compromise, and immediately upon system installation (e.g., default or vendor-supplied passwords)."

ITIO SOP – User Account Creation/Removal/Permission Procedures version 2.4, page 2, generally states ITIO's procedures for New Employee Account Creation, Current Employee Account Transfer, Departing Employees, Permissions Requests and Monthly Disable/Delete Process.

USB Port Control Access

NIST SP 800-53 Revision 3, section SI-3, page F-125, Recommended Security Controls for Federal Information Systems and Organizations, states that the organization "Employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code:

- Transported by electronic mail, electronic mail attachments, web accesses, [USB devices], or other common means; or
- Inserted through the exploitation of information system vulnerabilities …."

SAMHSA's Information Technology Security Program Policy states that "SAMHSA shall ensure appropriate physical security controls are in place to protect all Agency electronic media from unauthorized access. Electronic media may include disk drives, diskettes, internal and external hard drives, portable devices, backup media, removable media, and media containing sensitive information. Electronic media containing sensitive and privacy data shall be encrypted."

"All SAMHSA laptop computers shall be secured using a FIPS 140-2 compliant whole-disk encryption solution."

Substance Abuse and Mental Health Services Administration
SAMHSA
1 Choke Cherry Road • Rockville, MD 20857
www.samhsa.gov • 1-877-SAMHSA-7 (1-877-726-4727)

JUN 28 2013

TO: Director of Information System Auditor

FROM: Deputy Administrator for Operations

SUBJECT: 2013 Substance Abuse and Mental Health Services Administration's (SAMHSA) FISMA Audit Response

In response to the 2013 OIG FISMA Audit, attached is SAMHSA's response to the draft OIG FISMA Audit findings.

Mirtha R. Beadle

Attachment

SAMHSA

SAMHSA OIG AUDIT RESPONSE

Final Response

DTM IT Security

6/26/2013

This SAMHSA OIG Audit Response document identifies vulnerabilities discovered during the OIG Audit. This document highlights the detailed findings, OIG recommendations, and SAMHSA's detailed Plan of Action to remediate these items and improve overall security at SAMHSA and HHS.

Introduction

On May 31, 2013, the Division of Technology and Management (DTM) was provided with a draft copy of the Department of Health and Human Services' (HHS) Office of the Inspector General (OIG), Audit A-18-12-30420 report titled, *Information Security Weaknesses Poses Risk to Operations and Mission of SAMHSA.*

The report identifies five categories of vulnerabilities and makes 17 recommendations to improve security at HHS. SAMHSA concurs with the noted findings and has planned multiple activities to improve and/or remediate most of the items. Most of the suggested recommendations encourage SAMHSA to have more oversight and control on the outsourced network infrastructure and IT asset services managed by the Information Technology Infrastructure and Operations (ITIO).

The overall process of SAMHSA will be to work in collaboration with the ITIO to track progress against the plans that are in place to address the OIG recommendations, coordinate remediation efforts, and ensure appropriate tracking of outstanding items in their respective plans of action and milestones (POA&M). SAMHSA expects ITIO to be responsible for assessing their own risks with regards to each OIG finding and recommendation and to develop POA&Ms to properly address the recommendations. SAMHSA's POA&M will include items managed by the ITIO to ensure remediation efforts are uniformly tracked and properly mitigated. Additionally, SAMHSA will develop an internal audit review process by which to monitor and grade ITIO's performance.

OIG Findings and SAMHSA Status

This section contains a complete list of the recommended actions broken down by description, owner, concurrence and status. Status is further broken down into:

- Open: This task is still in the initial planning stages.
- In Progress: Plans for this task have begun to be implemented and are in development towards full mitigation or remediation.
- Complete: This task is complete.

SAMHSA will be sure to keep this Summary of findings current with the latest status for remediating the listed recommendations.

Table 2. HHS OIG MIR Response Summary

Finding	Description	Owner	Agree with Recommendation (Yes/No)	Status
OIG Recommendations				
R1	Implements the Departmental Property Management Information System (PMIS) in order to provide a continuous monitoring program to SAMHSA that will accurately account for all IT assets, and provide comprehensive reporting to the SAMHSA Chief Information Officer (CIO).	SAMHSA CISO	Yes	Open
R2	Updates inventory to include all computers and servers connecting to the SAMHSA network that are managed by ITIO. Employ controls that ensure an effective method for tracking computer inventory is implemented.	SAMHSA CISO	Yes	In Progress
R3	Upgrades or replace all servers with End-of-Life (EOL) operating systems to operating systems supported by the vendor.	SAMHSA CISO	Yes	In Progress
R4	Security team ensures that patch reports are accessible to SAMHSA's Chief Information Security Officer.	SAMHSA CISO	Yes	Open

Finding	Description	Owner	Agree with Recommendation (Yes/No)	Status
R5	Should reconcile SAMHSA's inventory and patch report data, at least monthly, to determine whether all assets are appropriately patched.	SAMHSA CISO	Yes	Open
R6	Update all computers and servers running out of date antivirus timestamp signatures.	SAMHSA CISO	Yes	Open
R7	Establish effective procedures to monitor and remediate computers with out-of-date timestamp signatures.	SAMHSA CISO	Yes	Open
R8	Document logging alerts that have been remediated.	SAMHSA CISO	Yes	Open
R9	Add the following processes to ITIO's Infrastructure Operations Standard Operating Procedure (SOP): – Follow-Up process for computers not in compliance with latest antivirus time stamps within SOP. – Process for server antivirus management.	SAMHSA CISO	Yes	Open
R10	Create naming conventions that include computer names that will define which organization it has been assigned to.	SAMHSA CISO	Yes	Open
R11	Disable accounts inactive greater than 60 days and subsequently delete accounts determined to be no longer needed greater than 90 days.	SAMHSA CISO	Yes	In Progress
R12	Delete user accounts of terminated employees.	SAMHSA CISO	Yes	Open
R13	Should disable, delete, or provide a waiver for the user account with a password status of "Not Required"	SAMHSA CISO	Yes	Open
R14	Periodically review access user control lists to determine if accounts are still needed.	SAMHSA CISO	Yes	Open
R15	Restrict personnel from connecting unauthorized USB devices to computers.	SAMHSA CISO	Yes	Open

Finding	Description	Owner	Agree with Recommendation (Yes/No)	Status
R16	Prevent sensitive data from being written to unauthorized/unencrypted USB devices.	SAMHSA CISO	Yes	Open
R17	Enforce the Department information security policy that restricts the connection of personally owned equipment to Department systems or networks.	SAMHSA CISO	Yes	Open

SAMHSA Detailed Plan of Action

SAMHSA acknowledges the importance of identifying potential security threats and will address all relevant identified weaknesses in a timely manner. Related to the Inspector General (IG) five categories of vulnerabilities SAMHSA plans to take the following steps of remediation:

Finding #1: ***Inventory Management*** *– The records given to us by ITIO had different totals of computers it managed for SAMHSA. Inventory was not tracked and managed effectively and therefore neither ITIO nor SAMHSA was able to account for all SAMHSA IT assets and ensure their security compliance*

Suggested Remediation Actions:

- *Implement the Departmental Property Management Information System (PMIS) in order to provide a continuous monitory program to SAMSHA that will accurately account for all IT assets, and provide comprehensive reporting to the SAMHSA Chief Information Officer (CIO.)*
- *Updates inventory to include all computers and servers connecting to the SAMHSA network that are managed by ITIO.*
- *Upgrades or replaces all servers with End-of-Life (EOL) operating systems to operating systems supported by the vendor.*

SAMHSA Response:

SAMHSA concurs with **Finding #1** and the OIG suggested remediation actions and plans to take the following steps of remediation:

1. SAMHSA team will meet with ITIO on bi-weekly basis to get status updates on the Implementation of Departmental Property Management Information System (PMIS) and provide assistance necessary to complete this task.
2. SAMHSA team will coordinate with ITIO to resolve IT assets inventory discrepancies. SAMHSA team will also work with ITIO on selecting one inventory management tool used by both teams to account for and report all IT assets.
3. SAMHSA team will ensure that the inventory management tool selected will provide operating system software information which will allow SAMHSA and ITIO to identify systems that are running operating systems that are no longer supported by the vendor and create a plan for updating these systems.

Finding #2: Patch ***Management*** *– SAMHSA did not ensure that ITIO had effectively implemented its patch management program for those devices managed by ITIO. We identified*

vulnerabilities within the SAMHSA network that if exploited could have led to unauthorized disclosure, modification, or non-availability of critical data.

Suggested Remediation Actions:

- *Security team ensures that patch reports are accessible to SAMHSA Chief Information Security officer.*
- *Should reconcile SAMHSA's inventory and patch report data, at least monthly, to determine whether all assets are appropriately patched.*

SAMHSA Response:

SAMHSA concurs with **Finding #2** and the OIG suggested remediation actions and plans to take the following steps of remediation:

1. SAMHSA team will request on a bi-weekly basis a patch implementation report from ITIO and will provide these reports to SAMHSA's Chief Information Security Officer (CISO) on a schedule that the CISO selects.
2. SAMHSA team will meet with ITIO on a bi-weekly/monthly basis to reconcile inventory, patching or antivirus compliance reports.

Finding #3: Antivirus *Management* *–ITIO and SAMHSA did not ensure that all of the SAMHSA computers and servers managed by ITIO had updated antivirus signatures.*

Suggested Remediation Actions:

- *Update all computers and servers running out of date antivirus timestamp signatures.*
- *Establish effective procedures to monitor and remediate computers with out-of-date timestamp signatures.*
- *Document logging alerts that have been remediated.*
- *Add the following processes to ITIO's Infrastructure Operations Standard Operating Procedure (SOP):*

  -Follow-up process for computers not in compliance with the latest antivirus time stamps within SOP.

  -Process for server antivirus management.

- *Create naming conventions that include computer names that will define which organization it has been assigned to.*

SAMHSA Response:

SAMHSA concurs with **Finding #3** and the OIG suggested remediation actions and plans to take the following steps of remediation:

1. SAMHSA team will request ITIO to provide reports on bi-weekly basis that details antivirus engine and signature timestamps for all ITIO owned and managed computers and servers used for SAMHSA's operations.
2. SAMHSA team will request ITIO create a plan of action for monitoring and remediating computers with out-of-date timestamp signatures.
3. SAMHSA team will request on a bi-weekly basis a report from ITIO detailing applicable security patch application on all ITIO owned and managed computers and servers used for SAMHSA's operations.
4. SAMHSA team will verify that ITIO's Infrastructure Operations Standard is updated with the following: Follow-up process for computers not in compliance with latest antivirus time stamps, Process for server antivirus management.
5. SAMHSA team will work with ITIO in creating naming conventions within Active Directory for all ITIO owned and managed computers and servers used for SAMHSA's operations.

Finding #4: Logical Access – *ITIO and SAMHSA did not implement an effective logical access control process for its user accounts and did not conduct sufficient reviews to ensure that only valid users had access to their information system.*

Suggested Remediation Actions:

- *Disable accounts inactive greater than 60 days and subsequently delete accounts determined to be no longer needed greater than 90 days.*
- *Delete user accounts of terminated employees.*
- *Should disable, delete, or provide a waiver for the user account with a password status of "Not Required."*
- *Periodically review access user control lists to determine if accounts are still needed.*

SAMHSA Response:

SAMHSA concurs with **Finding #4** and the OIG suggested remediation actions and plans to take the following steps of remediation:

1. SAMHSA team will coordinate a meeting with ITIO to ensure technical controls are implemented to disable accounts inactive greater than 60 days and subsequently delete accounts determined to be no longer needed greater than 90 days for all ITIO owned and managed computers and servers used for SAMHSA's operations.

2. SAMHSA team will coordinate a meeting with ITIO to review the process of deleting user accounts of terminated employees and ensure technical controls are implemented to enforce this process.
3. SAMHSA team will coordinate a meeting with ITIO to verify that all accounts with password status of "Not Required" are disabled, deleted, or a waiver has been provided for the user account and ensure technical controls are implemented to enforce this.
4. SAMHSA team will coordinate a meeting with ITIO to verify access user control list review is documented and performed periodically.

Finding #5: USB Port Control Access – *ITIO and SAMHSA did not have any technical controls to prevent unauthorized and unencrypted USB devices from connecting to SAMHSA computer.*

Suggested Remediation Actions:

- *Restrict personnel from connecting unauthorized USB devices to computer.*
- *Prevent sensitive data from being written to unauthorized /unencrypted USB devices.*
- *Enforce the Department information security policy that restricts the connection of personally owned equipment to Department systems or networks.*

SAMHSA Response:

SAMHSA concurs with **Finding #5** and the OIG suggested remediation actions and plans to take the following steps of remediation:

1. SAMHSA team will coordinate a meeting with ITIO to ensure technical controls are implemented to restrict personnel from connecting unauthorized USB devices to ITIO owned and managed computers and servers used for SAMHSA's operations.
2. SAMHSA team will coordinate a meeting with ITIO to ensure technical controls are implemented to prevent sensitive data from being written to unauthorized/unencrypted USB devices on ITIO owned and managed computers and servers used for SAMHSA's operations.
3. SAMHSA team will coordinate a meeting with ITIO to ensure technical controls are implemented to enforce HHS information security policy that restricts the connection of personally owned equipment to SAMHSA systems or networks.

Summary of SAMHSA Response:

In conclusion SAMHSA acknowledges it needs to strengthen its communication and collaboration with the ITIO. Most, if not all, of the suggested OIG recommendations require SAMHSA to communicate and have more visibility of the outsourced network services managed by the ITIO. SAMHSA appreciates the OIG review and will utilize the recommendations to ensure the continued confidentiality, integrity and availability of SAMHSA information and information assets.

In SAMHSA response to the OIG recommendations the common dynamic is the engagement in more recurring meetings. These meetings will be structured to repeat the same processes the OIG exercised that revealed the security findings. SAMHSA is confident that its planned responses will result in a more strengthened security program that is more vigilant and aware of the success of the network services provided. SAMHSA expects full cooperation and timely participation from the ITIO to remediate the suggested recommendations in a timely manner.