****

**SMART PORTAL**

**SECURITY TEST & EVALUATION (st&e)**

SMART THINK

April 2014

TABLE OF CONTENTS

[1. EXECUTIVE SUMMARY 1](#_Toc385501506)

[1.1. BACKGROUND 1](#_Toc385501507)

[1.2. SCOPE 1](#_Toc385501508)

[2. DETAILED FINDINGS 2](#_Toc385501509)

[3. FINDINGS MATRIX 3](#_Toc385501510)

# EXECUTIVE SUMMARY

Smart Think has engaged MJHS to perform an onsite comprehensive scope Federal Information Security Management Act (FISMA) assessment of the Smart Portal as part of the SMART THINK Certification and Accreditation (C&A) Program in order to define the security posture of the system’s infrastructure.

## BACKGROUND

The Smart Portal is a web-based application only accessible to smart Think employees that gives Smart Think staff a single point of access to the smart Think-provided data, documents, and applications available at the corporate level. The mission of the Portal is to offer: 1) an integrated environment for aggregating and centralizing the retrieval of information from both internal and external sources; 2) a convenient platform for exposing existing systems within a unified web environment irrespective of platform; 3) the facilitation of knowledge management and collaboration among employees and across organizations; and 4) facilitate the storage of employment personal information (name, address s and Telephone).

## SCOPE

The audit included a review of all SMART PORTAL policies and procedures related to the eighteen (18)-security control families listed below:

* Access Control (AC)
* Awareness and Training (AT)
* Audit and Accountability (AU)
* Certification, Accreditation and Security Assessments (CA)
* Configuration Management (CM)
* Contingency Planning (CP)
* Identification and Authentication (IA)
* Incident Response (IR)
* Maintenance (MA)
* Media Protection (MP)
* Physical and Environmental Protection (PE)
* Planning (PL)
* Personnel Security (PS)
* Program Management (PM)
* Risk Assessment (RA)
* System and Services Acquisition (SA)
* System and Communications Protection (SC)
* System and Information Integrity (SI)

# DETAILED FINDINGS

The following table contains assessment procedures, or steps, for assessing each of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 3 security controls. These procedures (Columns 1 through 3) are extracted directly from NIST SP 800-53 Revision 3. The table columns should be interpreted as follows:

* Control – indicates the security control that is being addressed (i.e. Access Control (AC)).
  + # – indicates the number of the security control (i.e. AC-1)
  + Step – indicates the procedural step associated with a security control #
* Procedure – detailed instructions to test the validity of each security control
* Assessment Result – detailed results of the assessment step are documented in this column. The description should contain enough detail (evidence) to provide assurance that the intent of the control is satisfactorily implemented.
* Pass/Fail/NA– indicates the results status of each assessment step.
* Ownership – indicates the organization the finding belongs to (SMART THINK, SMART PORTAL or both)

# FINDINGS MATRIX

| **Control** | **#** | **Step** | **Procedure** | **Assessment Result** | **Pass/Fail/NA** | **Ownership** | **Potential Validation** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| AC | 1 | 1 | Determine if:   (i) the organization develops and formally documents access control policy;   (ii) the organization access control policy addresses:  a. purpose;  b. scope;  c. roles and responsibilities;  d. management commitment;  e. coordination among organizational entities;  f. compliance;   (iii) the organization disseminates formal documented access control policy to elements within the organization having associated access control roles and responsibilities;   (iv) the organization develops and formally documents access control procedures;   (v) the organization access control procedures facilitate implementation of the access control policy and associated access controls;   (vi) the organization disseminates formal documented access control procedures to elements within the organization having associated access control roles and responsibilities;   (vii) the organization reviews/updates the access control policy and procedures within every three hundred sixty-five (365) days. | This control is inherited from Smart Think. | PASS | SMART THINK | Access Control Policy and Procedure |
| AC | 2 | 1 | Determine if:   (i) the organization manages information system accounts, including; - identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);  a. establishing conditions for group membership;  b. identifying authorized users of the information system and specifying access privileges;  c. requiring appropriate approvals for requests to establish accounts;  d. establishing, activating, modifying, disabling, and removing accounts;  e. specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;  f. notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes;  g. deactivating: (a) temporary accounts that are no longer required; and (b) accounts of terminated or transferred users;  h. granting access to the system based on: (a) a valid access authorization; (b) intended system usage; and (c) other attributes as required by the organization or associated missions/business functions;   (ii) the organization reviews information system accounts in accordance with the frequency specified below:  a. Review information system accounts within every one hundred eighty (180) days and require annual certification.   (iii) the organization meets all the requirements specified below:  a. Remove or disable default user accounts. Rename active default accounts.  b. Implement centralized control of user access administrator functions.  c. Regulate the access provided to contractors and define security requirements for contractors. | This control is inherited from Smart Think. | PASS | SMART THINK | List of recently disabled information system accounts along with the name of the individual associated with each account |
| AC | 2 | E7 | Determine if:   (i) the organization establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles;   (ii) the organization tracks and monitors privileged role assignments;   (iii) the organization inspects administrator groups, root accounts and other system related accounts on demand, but at least every fourteen (14) days to ensure that unauthorized accounts have not been created. | Based on interviews with the ISSO, elevated-privilege accounts are reviewed quarterly. However, the SMART PORTAL did not provide evidence, in the form of an audit/review log to verify, that elevated-privilege accounts are reviewed on a quarterly basis. | FAIL | SMART PORTAL |  |
| AC | 5 | 1 | Determine if:   (i) the organization separates duties of individuals as necessary, to prevent malevolent activity without collusion;   (ii) the organization documents separation of duties;   (iii) the organization implements separation of duties through assigned information system access authorizations.   (iv) the organization meets all the requirements specified below:  a. Ensure that audit functions are not performed by security personnel responsible for administering access control.  b. Maintain a limited group of administrators with access based upon the users' roles and responsibilities.  c. Ensure that critical mission functions and information system support functions are divided among separate individuals.  d. Ensure that information system testing functions (i.e., user acceptance, quality assurance, information security) and production functions are divided among separate individuals or groups.  e. Ensure that an independent entity, not the Business Owner, System Developer(s)/Maintainer(s), or System Administrator(s) responsible for the information system, conducts information security testing of the information system. | The system's different functions are programmatically separated between SMART THINK and the SMART PORTAL in an effort to eliminate possible conflicts of interests in the responsibilities and duties that have been assigned to individuals. In addition, based on interviews and the position descriptions received, the SMART PORTAL assigns duties and responsibilities that maintain separation of duties within the facility. | PASS | SMART PORTAL |  |
| AC | 6 | 1 | Determine if:   (i) the organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.   (ii) the organization meets all the requirements specified below:  a. Disable all file system access not explicitly required for system, application, and administrator functionality.  b. Contractors must be provided with minimal system and physical access, and must agree to and support the SMART THINK security requirements. The contractor selection process must assess the contractor's ability to adhere to and support SMART THINK security policy.  c. Restrict the use of database management utilities to only authorized database administrators. Prevent users from accessing database data files at the logical data view, field, or field-value level. Implement table-level access control.  d. Ensure that only authorized users are permitted to access those files, directories, drives, workstations, servers, network shares, ports, protocols, and services that are expressly required for the performance of job duties.  e. Disable all system and removable media boot access unless it is explicitly authorized by the CIO for compelling operational needs. If authorized, boot access is password protected. | SMART THINK employs the concept of least privilege as well as the SMART PORTAL. Each user is only granted the level of access that is required for them to complete their job functions. All file system access not explicitly required for system application and administrator functionality is disabled. Contractors and all general users must undergo training and adhere to SMART THINK security policies. Database administrators at both the SMART PORTAL and SMART THINK are the only personnel with elevated-privilege access to database data files. | PASS | SMART PORTAL | Access control policy and procedures |
| AC | 6 | E2 | Determine if:   (i) the organization defines the security functions or security-relevant information to which users of information system accounts, or roles, have access;   (ii) the organization requires that users of information system accounts, or roles, with access to organization-defined security functions or security-relevant information, use non-privileged accounts, or roles, when accessing other system functions;   (iii) the organization, if deemed feasible, audits and use of privileged accounts, or roles with access to organization-defined security functions or security-relevant information when assessing other system functions. | It is clearly defined which security functions and/or security information each user is able to access. Administrators are authorized to use their accounts only in support of functions that directly require elevated access such as monthly maintenance. These administrators are issued basic user accounts which are used to complete all other assigned tasks. | PASS | SMART PORTAL |  |
| AC | 17 | 1 | Determine if:   (i) the organization documents allowed methods of remote access to the information system;   (ii) the organization establishes usage restrictions and implementation guidance for each allowed remote access method;   (iii) the organization monitors for unauthorized remote access to the information system;   (iv) the organization authorizes remote access to the information system prior to connection;   (v) the organization enforces requirements for remote connections to the information system.   (vi) the organization meets all the requirements specified below:  a. Require callback capability with re-authentication to verify connections from authorized locations when the Medicare Data Communications Network (MDCN) or Multi Protocol Label Switching (MPLS) service network can not be used.  b. If e-authentication is implemented as a remote access solution or associated with remote access, refer to ARS Appendix D, E-authentication Standard. | The SMART PORTAL has no remote users. | N/A | SMART PORTAL |  |
| AC | 19 | E1 | Determine if the organization restricts the use of writable, removable media in SMART THINK information systems. | Based on an interview with the ISSO, the SMART PORTAL prohibits the use of writable, removable media in SMART THINK information systems. However, there is no existing policy that governs the use of writable, removable media. | FAIL | SMART PORTAL |  |
| AC | 19 | E2 | Determine if the organization prohibits the use of personally owned, removable media in SMART THINK information systems. | Based on an interview with the ISSO, the SMART PORTAL prohibits the use of personally owned, removable media in SMART THINK information systems. However, there is no existing policy that governs the use of personally owned, removable media. | FAIL | SMART PORTAL |  |
| AC | 19 | E3 | Determine if the organization prohibits the use of removable media in SMART THINK information systems when the media has no identifiable owner. | There is no existing policy that governs the use of removable media when the media has no identifiable owner. | FAIL | SMART PORTAL |  |
| AT | 1 | 1 | Determine if:   (i) the organization develops and formally documents security awareness and training policy;   (ii) the organization security awareness and training policy addresses:  a. purpose;  b. scope;  c. roles and responsibilities;  d. management commitment;  e. coordination among organizational entities, and compliance;   (iii) the organization disseminates formal documented security awareness and training policy to elements within the organization having associated security awareness and training roles and responsibilities;   (iv) the organization develops and formally documents security awareness and training procedures;   (v) the organization security awareness and training procedures facilitate implementation of the security awareness and training policy and associated security awareness and training controls;   (vi) the organization disseminates formal documented security awareness and training procedures to elements within the organization having associated security awareness and training roles and responsibilities;   (vii) the organization reviews/updates the security awareness and training policy and procedures within every three hundred sixty-five (365) days. | The SMART PORTAL SSP sufficiently addresses the security awareness and training procedures and references the SAT memo “Annual Smart Portal Security Training Requirements for All Users” issued annually by SMART THINK. In addition, the SSP addresses the frequency of refresher training, personnel required to take and conduct the training and the record retention requirements for training related documents. The SAT policy and procedure is reviewed and/or updated on an annual basis. | PASS | SMART PORTAL |  |
| AT | 2 | 1 | Determine if:   (i) the organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users and when required by system changes;   (ii) the organization defines in the security plan, explicitly or by reference, the frequency of refresher security awareness training and the frequency is at least annually;   (iii) the organization provides refresher security awareness training within every three hundred sixty-five (365) days. | SMART PORTAL provides basic security awareness training to all users and provides refresher training annually or as needed. The SMART PORTAL SSP states the frequency of the refresher training as annually. | PASS | SMART PORTAL |  |
| AT | 3 | 1 | Determine if:   (i) the organization provides role-based security-related training before authorizing access to the system or performing assigned duties, and when required by system changes;   (ii) the organization provides role-based security-related refresher training within every three hundred sixty-five (365) days thereafter;   (iii) the organization meets all the requirements specified below:  a. Require personnel with significant information security roles and responsibilities to undergo appropriate information system security training prior to authorizing access to SMART THINK networks, systems, and/or applications; when required by system changes; and refresher training within every three hundred sixty-five (365) days thereafter. | SMART THINK provides role-based security-related training to ISSO before authorizing access to the system or performing assigned duties. Continuous training is conducted via memos, monthly ISSO calls, and the annual Smart Portal conference that occurs in December. | PASS | SMART PORTAL |  |
| AT | 4 | 1 | Determine if:   (i) the organization documents and monitors individual SMART THINK information system security training activities including basic security awareness training and specific information system security training;   (ii) the organization retains individual training records for three (3) years. | Basic security awareness training is monitored and documented by the ISSO. Personnel security awareness training records are maintained for at least three years. | PASS | SMART PORTAL |  |
| CA | 2 | 1 | Determine if:   (i) the organization develops a security assessment plan for the information system;   (ii) the security assessment plan describes the scope of the assessment including:  a. security controls and control enhancements under assessment;  b. assessment procedures to be used to determine security control effectiveness;  c. assessment environment, assessment team, and assessment roles and responsibilities.   (iii) the organization meets all the requirements specified below:  a. A security assessment of all security controls must be conducted prior to issuing the initial authority to operate for all newly implemented systems.  b. The annual security assessment requirement mandated by OMB requires all SMART THINKRs attributable to a system or application to be assessed over a 3-year period. To meet this requirement, a subset of the SMART THINKRs shall be tested each year so that all security controls are tested during a 3-year period.  c. The Business Owner notifies the SMART THINK CISO within thirty (30) days whenever updates are made to system security authorization artifacts or significant role changes occur (e.g., Business Owner, System Developer/Maintainer, ISSO). | The SMART PORTAL has been provided a security assessment plan that is represented by the SMART THINK Information Security ARS as well as the Audit Findings Report produced by Axiom. The controls are assessed by the SMART PORTAL on an annual basis when updating the SSP. | PASS | SMART PORTAL |  |
| CA | 2 | E1 | Determine if the organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system. | An independent certification agent (MJHS) is employed by SMART THINK to conduct security assessments of the SMART PORTAL network. | PASS | SMART PORTAL |  |
| CA | 3 | 1 | Determine if:   (i) the organization identifies connections to external information systems (i.e., information systems outside of the authorization boundary);   (ii) the organization authorizes connections from the information system to external information systems through the use of Interconnection Security Agreements;   (iii) the organization documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated;   (iv) the organization monitors the information system connections on an ongoing basis to verify enforcement of security requirements.   (v) the organization meets the requirement(s) specified below:  a. Record each system interconnection in the System Security Plan (SSP) and Information Security (IS) Risk Assessment (RA) for the SMART THINK system that is connected to the remote location. | There are no external information systems connected to SMART PORTAL. | N/A | SMART PORTAL |  |
| CA | 5 | 1 | Determine if:   (i) the organization develops a plan of action and milestones for the information system within thirty (30) days of the final results for every internal/external audit/review or test;   (ii) the plan of action and milestones documents the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system;   (iii) the organization defines in the security plan, explicitly or by reference, the frequency of plan of action and milestone updates;   (iv) the organization updates and submits existing POA&M monthly until all the findings are resolved based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities. | Plan of action and milestones (POA&M) are created timely for the SMART PORTAL following the annual site visit audit. However, the SMART PORTAL does not update POA&M items monthly. | FAIL | SMART PORTAL |  |
| CM | 6 | E3 | Determine if :   (i) the organization incorporates detection of unauthorized, security-relevant configuration changes into the organizations incident response capability;   (ii) to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes. | An unauthorized modification in the configuration of the information system will be considered a security breach and therefore must be reported as an incident. As required by the Incident Response Procedures, all incidents must be reported immediately to the ISSO. The ISSO will report the incident to the Smart Portal Helpdesk and in-turn creates a Security Incident Ticket through Remedy. The Remedy ticket is SMART THINK's way of ensuring that these events are tracked, monitored, corrected, and available for historical purposes. | PASS | SMART PORTAL |  |
| CM | 8 | 1 | Determine if:   (i) the organization defines information deemed necessary to achieve effective property accountability;   (ii) the organization develops, documents, and maintains an inventory of information system components that:  a. accurately reflects the current information system;  b. is consistent with the authorization boundary of the information system;  c. is at the level of granularity deemed necessary for tracking and reporting;  d. includes organization-defined information deemed necessary to achieve effective property accountability;  e. is available for review and audit by designated organizational officials. | The SMART PORTAL updates the inventory of information system components by completing the HHS 22 Report through the Remedy System. The SMART PORTAL maintains a current inventory of the components of the information system, which is detailed in the 565 report that is produced by Remedy. | PASS | SMART PORTAL |  |
| CM | 8 | E1 | Determine if the organization updates the inventory of information system components as an integral part of component:   (i) installations;  (ii) removals;  (iii) information system updates. | Sufficient evidence was provided by the SMART PORTAL in the form of Remedy and ERB tickets to confirm that the SMART PORTAL updates the inventory of information system components within Remedy. | PASS | SMART PORTAL | Configuration management policy; configuration management plan; procedures addressing information system component inventory; information system inventory records; component installation records; other relevant documents or records |
| CM | 8 | E5 | Determine if the organization verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system. | The SMART PORTAL conducts an inventory of all components annually to determine that all components are accounted for based on the 565 Report. | PASS | SMART PORTAL |  |
| CP | 1 | 1 | Determine if:   (i) the organization develops and formally documents contingency planning policy;   (ii) the organization contingency planning policy addresses:  a. purpose;  b. scope;  c. roles and responsibilities;  d. management commitment;  e. coordination among organizational entities;  f. compliance;  (iii) the organization disseminates formal documented contingency planning policy to elements within the organization having associated contingency planning roles and responsibilities;   (iv) the organization develops and formally documents contingency planning procedures;   (v) the organization contingency planning procedures facilitate implementation of the contingency planning policy and associated contingency planning controls;   (vi) the organization disseminates formal documented contingency planning procedures to elements within the organization having associated contingency planning roles and responsibilities;   (vii) the organization reviews/updates the contingency planning policy and procedures within every three hundred sixty-five (365) days. | The SMART PORTAL-BCCP ver.3.2 dated April 3, 2013 details the current Contingency Plan of the SMART PORTAL. This document is maintained by the ISSO who is responsible for updating and reviewing the BCCP on an annual basis. The SMART PORTAL's BCCP is disseminated to all personnel with contingency plan responsibilities. | PASS | SMART PORTAL |  |
| CP | 2 | 1 | Determine if:   (i) the organization develops a contingency plan for the information system that:  a. identifies essential missions and business functions and associated contingency requirements;  b. provides recovery objectives, restoration priorities, and metrics;  c. addresses contingency roles, responsibilities, assigned individuals with contact information;  d. addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;  e. addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented;  f. is reviewed and approved by designated officials within the organization;   (ii) the organization defines key contingency personnel (identified by name and/or by role) and organizational elements designated to receive copies of the contingency plan;   (iii) the organization distributes copies of the contingency plan to organization-defined key contingency personnel and organizational elements. | SMART PORTAL BCCP, version 3.2, dated April 2013 contains all contingency plan elements as required. The BCCP is developed and revised to address updates, disseminated to key contingency personnel, reviewed and approved by designated personnel. The BCCP adequately assigns responsibilities to specific roles and key personnel have a valid understanding of what is required of them. | PASS | SMART PORTAL |  |
| CP | 2 | 2 | Determine if:   (i) the organization coordinates contingency planning activities with incident handling activities;   (ii) the organization defines the frequency of contingency plan reviews;   (iii) the organization reviews the contingency plan for the information system in accordance with the organization-defined frequency;   (iv) the organization revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution or testing;   (v) the organization communicates contingency plan changes to the key contingency personnel and organizational elements. | The SMART PORTAL did not provide evidence that incident handling functions are completed in collaboration with contingency planning tasks. It is also unclear what modifications have been made to CP procedures, training, and test exercises based on lessons learned from previous incidents. | FAIL | SMART PORTAL |  |
| CP | 2 | E1 | Determine if the organization coordinates the contingency plan development with other organizational elements responsible for related plans. | The SMART PORTAL coordinates the development and review of the contingency plan with members of the SMART PORTAL responsible for related plans. | PASS | SMART PORTAL |  |
| CP | 2 | E2 | Determine if the organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations. | The AR1-SMART PORTAL conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations. | PASS | SMART PORTAL |  |
| CP | 3 | 1 | Determine if:   (i) the organization provides initial contingency training to personnel with contingency roles and responsibilities with respect to the information system;   (ii) the organization defines in the security plan, explicitly or by reference, the frequency of refresher contingency training and the frequency is at least annually;   (iii) the organization provides refresher training within every three hundred sixty-five (365) days. | The SMART PORTAL does not conduct annual CP training, CP test exercises, or after action training. | FAIL | SMART PORTAL |  |
| CP | 4 | 1 | Determine if:   (i) the organization defines in the security plan, explicitly or by reference, the contingency plan tests and/or exercises to be conducted;   (ii) the organization defines in the security plan, explicitly or by reference, the frequency of contingency plan tests and/or exercises and the frequency is at least annually;   (iii) the organization tests/exercises the contingency plan using organization-defined tests/exercises within every three hundred sixty-five (365) days;   (iv) the organization reviews the contingency plan test/exercise results and takes corrective actions. | The SMART PORTAL does not conduct annual CP training, CP test exercises, or after action training. | FAIL | SMART PORTAL |  |
| CP | 4 | E1 | Determine if the organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans. | The SMART PORTAL does not conduct annual CP training, CP test exercises, or after action training. | FAIL | SMART PORTAL |  |
| CP | 6 | 1 | Determine if:   (i) the organization establishes an alternate storage site;   (ii) the organization initiates necessary alternate storage site agreements to permit the storage and recovery of information system backup information. | The SMART PORTAL has an alternate storage site agreement with Central Records Storage. Authorized personnel from Central Records Storage pick up backup tapes at the SMART PORTAL location on a weekly basis. Weekly tapes are returned to the SMART PORTAL after three weeks. | PASS | SMART PORTAL |  |
| CP | 6 | E1 | Determine if:   (i) the contingency plan identifies the primary storage site hazards;   (ii) the alternate storage site is separated from the primary storage site so as not to be susceptible to the same hazards identified at the primary site. | The BCCP outlines primary storage site hazards and the site is approximately 15 miles from the primary facility so as not to be susceptible to the same hazards identified. | PASS | SMART PORTAL |  |
| CP | 6 | E3 | Determine if:   (i) the organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster;   (ii) the organization outlines explicit mitigation actions for organization identified accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster. | The BCCP identifies potential accessibility problems (i.e. navigation to and from the facility) to the alternate storage site in the event of an area-wide disaster. They also outline the mitigation actions for identified accessibility problems to the alternate storage site. | PASS | SMART PORTAL |  |
| CP | 9 | 1 | Determine if:   (i) the organization backs up user-level information in accordance with the frequency specified in below:  a. Perform full backups weekly to separate media. Perform incremental or differential backups daily to separate media. Backups to include user-level and system-level information (including system state information). Three (3) generations of backups (full plus all related incremental or differential backups) are stored off-site. Off-site and on-site backups must be logged with name, date, time and action;   (ii) the organization backs up system-level information in accordance with the frequency specified;   (iii) the organization backs up information system documentation (including security-related information and other forms of data).   (iv) the organization meets the requirement(s) specified below:  a. (For PII only) Ensure that a current, retrievable, copy of PII is available before movement of servers. | The AR1-SMART PORTAL maintains only one weekly backup tape offsite at Central Records Storage (a bonded company) for two weeks, which is not sufficient based on the information system backup requirement of three (3) generations and a minimum of fifteen (15) backup tapes(full plus all related incremental or differential backups) stored off site. | FAIL | SMART PORTAL |  |
| CP | 9 | 2 | Determine if the organization protects the confidentiality and integrity of backup information at the storage location. | The SMART PORTAL has implemented the appropriate measures to protect the confidentiality of backup information; however, the integrity of backup media cannot be verified due to the lack of encryption . | FAIL | SMART PORTAL |  |
| CP | 9 | E1 | Determine if:   (i) the organization defines in the security plan, explicitly or by reference, the frequency of information system backup testing;   (ii) the organization conducts information system backup testing in accordance with organization-defined frequency to verify backup media reliability and information integrity. | The SMART PORTAL has implemented the appropriate measures to protect the confidentiality of backup information; however, the integrity of backup media cannot be verified due to the lack of encryption. | FAIL | SMART PORTAL | Information System Backup Test Results |
| CP | 10 | 1 | Determine if:   (i) the organization provides automated mechanisms and/or manual procedures for the recovery and reconstitution of the information system to known state after a disruption, compromise, or failure;   (ii) the organization provides for the recovery of the information system after a failure or other contingency in a trusted, secure, and verifiable manner.   (iii) the organization meets all the requirements specified below:  a. Secure information system recovery and reconstitution includes, but not limited to:     • Reset all system parameters (either default or organization-established),     • Reinstall patches,     • Reestablish configuration settings,     • Reinstall application and system software, and     • Fully test the system. | Procedures for system reconstitution are available in the SMART PORTAL Infrastructure Operations and Support Manual, version 5.2, dated May 2011, the SMART PORTAL Infrastructure IT Administrator Manual, version 5.2, dated May 2011, the SMART PORTAL BCCP, as well as various aspects of the Monthly Network Maintenance (MNM) procedures requested by SMART THINK. Additionally, restoration of data from backup media is tested by the ISSO to verify success/failure of the backups; which are then recorded into the monthly backup logs created. | PASS | SMART PORTAL |  |
| CP | 10 | E2 | Determine if the information system implements transaction recovery for systems that are transaction-based. |  | N/A | SMART PORTAL |  |
| CP | 10 | E3 | Determine if:   (i) the organization defines in the security plan, explicitly or by reference, the circumstances that can inhibit recovery and reconstitution of the information system to a known state;   (ii) the organization provides compensating security controls for organization-defined circumstances that can inhibit recovery and reconstitution of the information system to a known state. | The SMART PORTAL BCCP defines the possible obstacles that may inhibit the resumption of normal operations for SMART PORTAL. It also defines the mitigation actions that would be required in the event of a disruption of mission critical functions. | PASS | SMART PORTAL |  |
| IA | 5 | E3 | Determine if:   (i) the organization defines the types of and/or specific authenticators for which the registration process must be carried out in person before a designated registration authority with authorization by a designated organizational official;   (ii) the organization requires that the registration process to receive hardware tokens be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor). | Interviews with the SMART PORTAL confirmed that authenticators are provided in person to new users before joining SMART PORTAL. In addition, hardware tokens are not issued. | PASS | SMART PORTAL |  |
| IR | 1 | 1 | Determine if:   (i) the organization develops and disseminates and formally documents incident response policy;   (ii) the organization's incident response policy addresses:  a. purpose;  b. scope;  c. roles and responsibilities;  d. management commitment;  e. coordination among organizational entities;  f. compliance;   (iii) the organization disseminates formal documented incident response policy to elements within the organization having associated incident response roles and responsibilities;   (iv) the organization develops and formally documents incident response procedures;   (v) the organization's incident response procedures facilitate the implementation of the incident response policy, and associated incident response controls;   (vi) the organization disseminates formal documented incident response procedures to elements within the organization having associated incident response roles and responsibilities;   (vii) the organization reviews/updates the incident response policy and procedures within every three hundred sixty-five (365) days. | The SMART PORTAL's incident response procedures are outlined in the SMART PORTAL SSP, distributed to the appropriate personnel and updated every 365 days. | PASS | SMART THINK SMART PORTAL |  |
| IR | 2 | 1 | Determine if:   (i) the organization identifies personnel with incident response roles and responsibilities with respect to the information system;   (ii) the organization provides incident response training to personnel with incident response roles and responsibilities with respect to the information system;   (iii) incident response training material addresses the procedures and activities necessary to fulfill identified organizational incident response roles and responsibilities;   (iv) the organization defines in the security plan, explicitly or by reference, the frequency of refresher incident response training and the frequency is at least annually;   (v) the organization provides refresher incident response training in accordance with organization-defined frequency. | The SMART PORTAL does not conduct annual incident response training, IR test exercises, or after-action training to determine the effectiveness of their IR procedures. | FAIL | SMART PORTAL |  |
| IR | 3 | 1 | Determine if:   (i) the organization defines incident response tests/exercises;   (ii) the organization defines in the security plan, explicitly or by reference, the frequency of incident response tests/exercises and the frequency is at least annually;   (iii) the organization tests/exercises the incident response capability for the information system using organization-defined tests/exercises in accordance with organization-defined frequency;   (iv) the organization documents the results of incident response tests/exercises;   (v) the organization determines the effectiveness of the incident response capability. | The SMART PORTAL does not conduct annual incident response training, IR test exercises, or after-action training to determine the effectiveness of their IR procedures. | FAIL | SMART PORTAL |  |
| IR | 4 | 1 | Determine if:   (i) the organization implements an incident handling capability for security incidents that includes:  a. preparation;  b. detection and analysis;  c. containment;  d. eradication;  e. recovery;   (ii) the organization coordinates incident handling activities with contingency planning activities;   (iii) the organization incorporates the lessons learned from ongoing incident handling activities into:  a. incident response procedures;  b. training;  c. testing/exercises;   (iv) the organization implements the resulting changes to incident response procedures, training and testing/exercise accordingly.   (v) the organization meets all the requirements specified below:  a. Document relevant information related to a security incident according to SMART THINK Information Security Incident Handling and Breach Notification Procedures.  b. Preserve evidence through technical means, including secured storage of evidence media and "write" protection of evidence media. Use sound forensics processes and utilities that support legal requirements. Determine and follow chain of custody for forensic evidence.  c. Identify vulnerability exploited during a security incident. Implement security safeguards to reduce risk and vulnerability exploit exposure. | The SMART PORTAL did not provide evidence that incident handling functions are completed in collaboration with contingency planning tasks. It is also unclear what modifications have been made to CP procedures, training, and test exercises based on lessons learned from previous incidents. | FAIL | SMART THINK SMART PORTAL |  |
| IR | 5 | 1 | Determine if the organization tracks and documents information system security incidents. | The SMART PORTAL uses the Remedy system as the repository for tracking and documenting all security incidents. | PASS | SMART THINK SMART PORTAL |  |
| IR | 6 | 1 | Determine if:   (i) the organization requires personnel to report suspected security incidents to the organizational incident response capability within the timeframe established in the current SMART THINK Information Security Incident Handling and Breach Analysis/Notification Procedure;   (ii) the organization reports security incident information to designated authorities. | As stated in the Smart Portal Incident Response Procedures, version 5.1, dated August 2010, all Smart Portal users are responsible for immediately reporting actual or suspected security intrusions, incidents, events, violations, or breaches to appropriate designated authorities (ISSO, Alternate ISSO, or the Smart Portal Help Desk). Immediately after a suspected security event discovery, a ticket must be created and the Smart Portal Security team must be notified. The ISSO has one business day to complete the Incident Response Form and submit this form to the Smart Portal Help Desk. | PASS | SMART PORTAL |  |
| IR | 6 | E1 | Determine if the organization employs automated mechanisms to assist in the reporting of security incidents. | The SMART PORTAL uses the Remedy system to track, document and assist in reporting security incidents. | PASS | SMART PORTAL |  |
| MA | 1 | 1 | Determine if:   (i) the organization develops and formally documents system maintenance policy;   (ii) the organization's information system maintenance policy addresses:  a. purpose;  b. scope;  c. roles and responsibilities; management commitment;  d. coordination among organizational entities;  e. compliance;   (iii) the organization disseminates formal documented system maintenance policy to elements within the organization having associated system maintenance roles and responsibilities;   (iv) the organization develops and formally documents system maintenance procedures;   (v) the organization system maintenance procedures facilitate implementation of the system maintenance policy and associated system maintenance controls;   (vi) the organization disseminates formal documented system maintenance procedures to elements within the organization having associated system maintenance roles and responsibilities;   (vii) the organization reviews/updates the information system maintenance policy and procedures within every three hundred sixty-five (365) days. | The SMART PORTAL SSP defines the maintenance procedures that must be followed by the SMART PORTAL and the individual responsible for carrying out the activities. The SSP is distributed to the appropriate personnel and updated every 365 days. | PASS | SMART THINK SMART PORTAL |  |
| MA | 2 | 1 | Determine if:   (i) the organization schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;   (ii) the organization controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;   (iii) the organization requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;   (iv) the organization sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;   (v) the organization checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.   (vi) the organization meets all the requirements below:  a. (For PII only) In facilities where PII is stored or accessed, document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks). | All onsite maintenance activities are tracked and documented through the use of various logs maintained by the ISSO. Employees with elevated accounts are authorized to conduct monthly maintenance. Outside Maintenance personnel and/or third party vendors are escorted at all times, and all equipment is tested following any repair to confirm it is functioning properly. Removal of any component requires approval from the SMART THINK help desk. | PASS | SMART PORTAL |  |
| MA | 2 | E1 | Determine if the organization maintains maintenance records for the information system that include:   (i) date and time of maintenance;   (ii) name of the individual performing the maintenance;   (iii) name of escort, if necessary; description of the maintenance performed; and   (iv) list of equipment removed or replaced (including identification numbers, if applicable). | The SMART PORTAL maintains maintenance records for the information system that are reviewed to verify date, time of maintenance, name of individual performing maintenance, name of escort if necessary, description of maintenance performed, and a list of any equipment removed or replaced. All documentation for maintenance actions is maintained in the Remedy ticket associated with the maintenance task performed . In addition, the front desk and server room visitor's sign in sheets document all maintenance personnel and activities. | PASS | SMART PORTAL |  |
| MA | 4 | E3 | Determine if:   (i) the organization requires and ensures non-local maintenance and diagnostic services from an information system that implements a level of security at least as high as the level of security implemented on the information system being serviced; or   (ii) the organization removes the component to be serviced from the information system and prior to non-local maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities;   (iii) the organization after the removed component service is performed, inspects and sanitizes the component (with regard to potentially malicious software and surreptitious implants) before reconnecting to the information system. | SMART THINK performs and approves all remote diagnostic and maintenance services. No other vendor has access to perform these services. No equipment is removed from the SMART PORTAL location to perform maintenance. It is all performed on-site and supervised by authorized designated personnel. | PASS | SMART PORTAL |  |
| MA | 5 | 1 | Determine if:   (i) the organization establishes a process for maintenance personnel authorization;   (ii) the organization maintains a current list of authorized maintenance organizations or personnel;   (iii) personnel performing maintenance on the information system either have the required access authorizations or are supervised by designated organizational personnel with the required access authorizations and technical competence deemed necessary to supervise information system maintenance. | Monthly Network Maintenance occurs on the third weekend of each month. The SMART PORTAL has established a process for authorized personnel with elevated accounts to perform maintenance. In addition, all authorized personnel listed are cross-referenced with the access control list to verify an active status. | PASS | SMART PORTAL |  |
| MP | 1 | 1 | Determine if:   (i) the organization develops and formally documents media protection policy;   (ii) the organization's media protection policy addresses:  a. purpose;  b. scope;  c. roles and responsibilities;  d. management commitment;  e. coordination among organizational entities;  f. compliance;   (iii) the organization disseminates formal documented media protection policy to elements within the organization having associated media protection roles and responsibilities;   (iv) the organization develops and formally documents media protection procedures;   (v) the organization's media protection procedures facilitate the implementation of the media protection policy, and associated media protection controls;   (vi) the organization disseminates formal documented media protection procedures to elements within the organization having associated media protection roles and responsibilities.    (vii) the organization reviews/updates the media protection policy and procedures within every three hundred sixty-five (365) days.   (viii) the organization meets all the requirements below:  a. (For PII only) Semi-annual inventories of magnetic tapes containing PII are conducted. The organization accounts for any missing tape containing PII by documenting the search efforts and notifying the tape initiator of the loss. | The SMART PORTAL SSP includes the following media protection procedures:    • Backup media procedures    • Media labeling and marking    • Procedures for transporting media off-site    • Security measures implemented to protect on-site media including PII    • Security measures in place to protect media transported outside of the facility    • Media sanitization/destruction.  Semi-annual inventories of magnetic tapes containing PII are not conducted by the SMART PORTAL. | FAIL | SMART PORTAL |  |
| MP | 2 | 1 | Determine if:   (i) the organization defines:  a. digital and non-digital media requiring restricted access;  b. individuals authorized to access the media;  c. security measures taken to restrict access;  (ii) the organization restricts access to organization-defined information system media to organization-defined authorized individuals using organization-defined security measures. | Based on interviews and observation, only authorized users are allowed to access the information system's media, which is located in the data center and/or medical records room. An authorized personnel list is maintained and checked frequently for privileged-elevated accounts and regular users to ensure all personnel are active. Security measures such as badge readers with corresponding proximity cards, and a fireproof safe are used to restrict access to the media. | PASS | SMART PORTAL |  |
| MP | 2 | E1 | Determine if:   (i) the organization employs automated mechanisms to restrict access to media storage areas;   (ii) the organization employs automated mechanisms to audit access attempts and access granted to media storage areas. | The IT office where the backup tapes are kept and the data centerare protected by key locks. Keys locks are manual and do not provide an audit trail of the access history. As a result, the SMART PORTAL is unable to conduct an audit to uncover access attempts and any access granted to the media storage areas. | FAIL | SMART PORTAL |  |
| MP | 3 | 1 | Determine if:   (i) the organization defines removable media types and information system output that require marking;   (ii) the organization marks removable media and information system output in accordance with organizational policies and procedures, indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information;   (iii) the organization defines:  a. removable media types and information system output exempt from marking;  b. controlled areas designated for retaining removable media and information output exempt from marking;   (iv) removable media and information system output exempt from marking remain within designated controlled areas. | The SMART THINK Media Policy outlines the media types and hardware that are exempt from external marking. The SMART PORTAL marks all information systems output using the following criteria:    • Do not copy or distribute    • Sensitive Information    • Special Handling Required | PASS | SMART PORTAL | Media Protection Policy, Data Classification policy |
| MP | 4 | 1 | Determine if:   (i) the organization defines:  a. types of digital and non-digital media physically controlled and securely stored within designated controlled areas;  b. controlled areas designated to physically control and securely store the media;  c. security measures to physically control and securely store the media within designated controlled areas;   (ii) the organization physically controls and securely stores SMART THINK information system media within organization-defined controlled areas using organization-defined security measures;   (iii) the organization protects SMART THINK information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures;   (iv) the organization meets all the requirements below:  a. (For PII only) Evaluate employing an approved method of cryptography (see SC-13) to protect PII at rest, consistent with NIST SP 800-66 guidance.  b. (For PII only) If PII is recorded on magnetic media with other data, it should be protected as if it were entirely personally identifiable information. | Entry to the IT office where the backup tapes are kept and the data centerare protected by key locks. Keys locks are manual and do not provide an audit trail of the access history for the media storage areas. | FAIL | SMART PORTAL |  |
| MP | 5 | 1 | Determine if:   (i) the organization protects and controls digital and non-digital media containing SMART THINK sensitive information during transport outside of controlled areas using cryptography and tamper evident packaging and (a) if hand carried, using securable container (e.g., locked briefcase) via authorized personnel, or (b) if shipped, track able with receipt by commercial carrier;   (ii) the organization maintains accountability for information system media during transport outside of controlled areas;   (iii) the organization identifies personnel authorized to transport information system media outside of controlled areas;   (iv) the organization restricts the activities associated with transport of information system media to authorized personnel.   (v) the organization meets all the requirements specified requirements below:  a. (For PII only) Protect and control PII media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel. PII must be in locked cabinets or sealed packing cartons while in transit.  b. (For FTI only) Organizations are not allowed to make further disclosures of FTI to their agents or to a contractor unless authorized by statute. (See IRS Pub. 1075, sect. 11.1 and 11.7 | The backup tapes are picked up by Central Records Storage (a bonded company) in a locked, portable case. However, backup tapes are unencrypted during transport. | FAIL | SMART PORTAL |  |
| MP | 5 | E2 | Determine if the organization documents activities associated with the transport of information system media. | Based on interviews and examination of artifacts collected, the SMART PORTAL documents the personnel (both SMART PORTAL and alternate storage site) that transport media, the date of pickup and drop-off, and the media being transported. | PASS | SMART PORTAL |  |
| MP | 5 | E4 | Determine if the organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas. | The backup tapes are picked up by Central Records Storage (a bonded company) in a locked, portable case. However, backup tapes are unencrypted during transport. | FAIL | SMART PORTAL |  |
| MP | 6 | 1 | Determine if:   (i) the organization sanitizes information system media both digital and non digital prior to:  a. disposal;  b. release out of organizational control; or  c. release for reuse;  (ii) the organization employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.   (iii) the organization meets all the requirements specified in the applicable implementation standard(s).  a. Finely shred, using a minimum of cross-cut shredding, hard-copy documents, using approved equipment, techniques, and procedures.  b. (For FTI only) FTI must never be disclosed to an agency's agents or contractors during disposal unless authorized by the Internal Revenue Code. Generally, destruction should be witnessed by an agency employee.  c. (For PII only) Authorized employees of the receiving entity must be responsible for securing magnetic tapes/cartridges before, during, and after processing, and they must ensure that the proper acknowledgment form is signed and returned. Inventory records must be maintained for purposes of control and accountability. Tapes containing PII, any hard-copy printout of a tape, or any file resulting from the processing of such a tape will be recorded in a log that identifies:     • date received     • reel/cartridge control number contents     • number of records, if available     • movement, and     • if disposed of, the date and method of disposition. | The SMART PORTAL follows sanitization instructions in accordance with SMART THINK guidance. All digital and non-digital media is stored in a secure location prior to sanitization and disposal. The SMART PORTAL employs J&L Paper Shredding Co (a bonded company) to sanitize and destroy all digital and non-digital media. Upon completion, a certificate of destruction is provided to the ISSO for record keeping. | PASS | SMART PORTAL |  |
| MP | 6 | E1 | Determine if the organization tracks, documents, and verifies media sanitization and disposal actions. | Based on interviews and examination of artifacts collected, the AR1-SMART PORTAL documents all media scheduled for decommission. The SMART PORTAL records, for sanitization and disposal, the date, contents, and the personnel or company responsible including signatures. | PASS | SMART PORTAL |  |
| MP | 6 | E2 | Determine if:   (i) the organization defines the frequency for testing sanitization equipment and procedures to verify correct performance;   (ii) the organization tests sanitization equipment and procedures to verify correct performance in accordance with organization-defined frequency. | The SMART PORTAL does not utilize personal/corporate sanitization (shredder/CD/degauzer) equipment for the purpose of sanitizing SMART PORTAL related media. | N/A | SMART PORTAL |  |
| MP | 6 | E6 | Determine if the organization implements the media destruction process for information system media that cannot be sanitized. | The SMART PORTAL destroys any media containing sensitive information that cannot be sanitized. The SMART PORTAL employs J&L Paper Shredding Co (a bonded company) to sanitize and destroy all digital and non-digital media. Upon completion, a certificate of destruction is provided to the ISSO for record keeping. | PASS | SMART PORTAL |  |
| PE | 1 | 1 | Determine if:   (i) the organization develops and formally documents physical and environmental protection policy;   (ii) the organization's physical and environmental protection policy addresses:  a. purpose;  b. scope;  c. roles and responsibilities;  d. management commitment;  e. coordination among organizational entities;  f. compliance;   (iii) the organization disseminates formal documented physical and environmental protection policy to elements within the organization having associated physical and environmental protection roles and responsibilities;   (iv) the organization develops and formally documents physical and environmental protection procedures;   (v) the organization physical and environmental protection procedures facilitate implementation of the physical and environmental protection policy and associated physical and environmental protection controls;   (vi) the organization disseminates formal documented physical and environmental protection procedures to elements within the organization having associated physical and environmental protection roles and responsibilities;   (vii) the organization reviews/updates the physical and environmental protection policy and procedures within every three hundred sixty-five (365) days. | The physical and environmental protection procedures are highlighted in the SMART PORTAL SSP. | PASS | SMART PORTAL |  |
| PE | 2 | 1 | Determine if:   (i) the organization identifies areas within the facility that are publicly accessible;   (ii) the organization develops and keeps current lists of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);   (iii) the organization issues authorization credentials (e.g., badges, identification cards, smart cards).   (iv) the organization reviews and approves the access list and authorization credentials at least once every one hundred eighty (180) days removing from the access list personnel no longer requiring access.  a. Review and approve lists of personnel with authorized access to facilities containing information systems at least once every one hundred eighty (180) days.   (v) the organization meets the requirement(s) specified below:  a. (For PII only) Create a restricted area, security room, or locked room to control access to areas containing PII. These areas will be controlled accordingly. | There are no publicly accessible areas within the SMART PORTAL’s suite. All PII is located in the medical records room, which complies with the two (2) barrier access control requirement. Physical access requests are submitted by the hiring manager to Westfield (the building management company) using a badge application form. Westfield issues the access badges for all employees in the building. However, evidence was not provided confirming that the SMART PORTAL reviews the physical access list every one hundred eighty (180) days, as required. | FAIL | SMART PORTAL |  |
| PE | 3 | 1 | Determine if:   (i) the organization enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible);   (ii) the organization verifies individual access authorizations before granting access to the facility;   (iii) the organization controls entry to the facility containing the information system using physical access devices (e.g., keys, locks, combinations, card readers) and/or guards;   (iv) the organization controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk;   (v) the organization secures keys, combinations, and other physical access devices;   (vi) the organization inventories physical access devices within every three hundred sixty-five (365) days;   (vii) the organization changes combinations and keys periodically; and when keys are lost, combinations are compromised, or individuals are transferred or terminated.   (viii) the organization meets all the requirements specified below:  a. Control data center/facility access by use of door and window locks, and security personnel or physical authentication devices, such as biometrics and/or smart card/PIN combination.  b. Store and operate servers in physically secure environments, and grant access to explicitly authorized personnel only. Access is monitored and recorded.  c. Restrict access to grounds/facilities to authorized persons only.  d. (For PII only) Require two barriers to access PII under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container. Protected information must be containerized in areas where other than authorized employees may have access afterhours. | The IT office where the backup tapes are kept and data centerare protected by key locks. Keys locks are manual and do not provide an audit trail of the access history. As a result, the SMART PORTAL is unable to conduct an audit to uncover access attempts and any access granted to the media storage areas.  The SMART PORTAL utilizes a badge reader system to gain access to the facility. Westfield is responsible for the badge access and key locks within the building. Key locks are utilized to access the offices. Westfield retains the extra keys, and conducts the key inventory. Westfield security guards are notified if keys are lost, stolen, or missing and changes are then made to the locks. However, evidence was not provided that confirm the SMART PORTAL conducts key inventories on a quarterly basis.  The area containing PII is compliant regarding the two barrier access requirement (i.e. access badge into case review area where only authorized personnel are allowed). | FAIL | SMART PORTAL |  |
| PE | 4 | 1 | Determine if:   (i) the organization controls physical access to information system distribution and transmission lines within organizational facilities.   (ii) the organization meets all the requirements specified below:  a. Permit access to telephone closets and information system distribution and transmission lines within organizational facilities only to authorized personnel.  b. Disable any physical ports (e.g., wiring closets, patch panels, etc) not in use. | The SMART PORTAL controls the physical access to the information system distribution and transmission lines. Only authorized personnel are allowed to access the data center, which is controlled via a badge reader and corresponding proximity cards. All physical ports (e.g., wiring, closets, patch panels, etc) not in use have been disabled. The telephone lines are also in a restricted area. Access to the Demark is controlled by badge access. | PASS | SMART PORTAL |  |
| PE | 5 | 1 | Determine if the organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output. | Upon examination, the SMART PORTAL controls physical access to information system output by arranging the monitors to face away from unauthorized viewing. | PASS | SMART PORTAL |  |
| PE | 6 | 1 | Determine if:   (i) the organization monitors physical access to the information system to detect and respond to physical security incidents;   (ii) the organization reviews physical access logs weekly;   (iii) the organization coordinates results of reviews and investigations with the organization's incident response capability. | The IT office where the backup tapes are kept and data centerare protected by key locks. Keys locks are manual and do not provide an audit trail of the access history for the data centerand the IT office. As a result, the SMART PORTAL is unable to conduct an audit to uncover access attempts and any access granted to the media storage areas.  The SMART PORTAL monitors physical access to the information system with badge readers for authorized personnel. All visitors must be processed and issued a visitor's badge. Entry to the information system is restricted and visitors must be escorted. Upon entry, all visitors must sign a Visitor's Log. Security guards patrol and protect the building 24 hours a day. Video cameras are installed throughout the facility and at the SMART PORTAL's suite. The SMART PORTAL is required to review physical access logs and video surveillance footage on a weekly basis. However, evidence was not provided to confirm that this review is completed. | FAIL | SMART PORTAL |  |
| PE | 6 | E1 | Determine if the organization monitors real-time physical intrusion alarms and surveillance equipment. | The SMART PORTAL is equipped with real-time physical intrusion alarms and motion detectors. Sensors are imbedded in all entrance/exit doors that will trigger an alarm if access is gained by force. In addition, the SMART PORTAL is equipped with surveillance cameras that cover all critical areas, entrances, and exits. However, the SMART PORTAL does not employ glass breakage sensors. | FAIL | SMART PORTAL |  |
| PE | 7 | 1 | Determine if the organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible. | Westfield and the SMART PORTAL authenticates visitors by requesting the visitor to show proper identification (government issued), sign the visitor log, and receive a visitor badge before authorizing access to the facility. However, not all data fields of the visitor’s log are populated. In addition, the SMART PORTAL does not audit and close the visitors' log every month. | FAIL | SMART PORTAL |  |
| PE | 7 | E1 | Determine if the organization escorts visitors and monitors visitor activity, when required. | The Westfield receptionist notifies the appropriate SMART PORTAL personnel of the visitor. The SMART PORTAL personnel reports to the lobby and the visitor is escorted to the facility. Visitor activity is monitored when required. | PASS | SMART PORTAL |  |
| PE | 8 | 1 | Determine if:   (i) the organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);   (ii) the organization closes and reviews the visitor access records monthly. | Westfield and the SMART PORTAL authenticates visitors by requesting the visitor to show proper identification (government issued), sign the visitor log, and receive a visitor badge before authorizing access to the facility. However, not all data fields of the visitor’s log are populated. In addition, the SMART PORTAL does not audit and close the visitors' log every month. | FAIL | SMART PORTAL |  |
| PE | 9 | 1 | Determine if:   (i) the organization protects power equipment and power cabling for the information system from damage and destruction.   (ii) the organization meets the requirement(s) specified below:  a. Permit only authorized maintenance personnel to access infrastructure assets, including power generators, HVAC systems, cabling, and wiring closets. | The AR1-SMART PORTAL protects power equipment and power cabling for the information system from damage and destruction. Only authorized maintenance personnel are permitted to access infrastructure assets. | PASS | SMART PORTAL |  |
| PE | 10 | 1 | Determine if:   (i) the organization provides the capability of shutting off power to the information system or individual system components in emergency situations;   (ii) the organization defines the location of emergency shutoff switches or devices by information system or system component;   (iii) the organization places emergency shutoff switches or devices in an organization-defined location by information system or system component to facilitate safe and easy access for personnel   (iv) the organization protects the emergency power shutoff capability from unauthorized activation. | There is an emergency power shutoff switch housed in the data center which provides the SMART PORTAL with the capability to shut off power to the information system or individual system components in emergency situations. | PASS | SMART PORTAL |  |
| PE | 11 | 1 | Determine if the organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss. | Westfield has a short-term uninterruptible power supply (UPS) installed on the SMART PORTAL rack located in the data center that can supply power for at least 40 minutes. In addition, Westfield has installed a 3.5 mega watt power generator that will fail-over to provide redundant power to the entire building. Westfield maintains and tests the generators annually. | PASS | SMART PORTAL |  |
| PE | 12 | 1 | Determine if:   (i) the organization employs automatic emergency lighting for the information system that activates in the event of a power outage or disruption;   (ii) the organization employs automatic emergency lighting for the information system that covers emergency exits and evacuation routes within the facility;   (iii) the organization maintains the automatic emergency lighting for the information system. | The emergency lighting is provided by the back-up generators. The generators restore 100% power to the data center and the entire building. Westfield maintains and tests the generators annually. | PASS | SMART PORTAL |  |
| PE | 13 | 1 | Determine if:   (i) the organization employs fire suppression and detection devices/systems for the information system that are supported by an independent energy source;   (ii) the organization maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source. | The SMART PORTAL is equipped with fire protection devices such as manual pull down fire alarms, a sprinkler system, fire extinguishers, smoke detectors, and strobe lights. Westfield (the facility management company) has contracted Simplex Grinnell to manage and maintain (including all annual testing) the building fire protection system. The SMART PORTAL’s fire detection devices will activate automatically and notify Simplex Grinnell personnel, who will in turn call Golding Living’s security team, and the fire department in the event of a fire. Westfield provides the space for all information systems in the data center. However, the SMART PORTAL does not employ a fire suppression device within the data center (e.g., FM200). | FAIL | SMART PORTAL |  |
| PE | 13 | E1 | Determine if the organization employs fire detection devices/systems for the information system that, without manual intervention, activate automatically and notify the organization and emergency responders in the event of a fire. | The SMART PORTAL is equipped with fire protection devices such as manual pull down fire alarms, sprinkler system, fire extinguishers, smoke detectors, and strobe lights. Westfield (the facility management company) has contracted Simplex Grinnell to manage and maintain (including all annual testing) the building fire protection system. The SMART PORTAL’s fire detection devices will activate automatically and notify Simplex Grinnell personnel, who will in turn call Golding Living’s security team, and the fire department in the event of a fire. | PASS | SMART PORTAL |  |
| PE | 13 | E2 | Determine if the organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to the organization and emergency responders. | The SMART PORTAL is equipped with fire protection devices such as manual pull down fire alarms, a sprinkler system, fire extinguishers, smoke detectors, and strobe lights. Westfield (the facility management company) has contracted Simplex Grinnell to manage and maintain (including all annual testing) the building fire protection system. The SMART PORTAL’s fire detection devices will activate automatically and notify Simplex Grinnell personnel, who will in turn call Golding Living’s security team, and the fire department in the event of a fire. Westfield provides the space for all information systems in the data center. However, the SMART PORTAL does not employ a fire suppression device within the data center (e.g., FM200). | FAIL | SMART PORTAL |  |
| PE | 13 | E3 | Determine if the organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis. | The SMART PORTAL is equipped with fire protection devices such as manual pull down fire alarms, a sprinkler system, fire extinguishers, smoke detectors, and strobe lights. Westfield (the facility management company) has contracted Simplex Grinnell to manage and maintain (including all annual testing) the building fire protection system. The SMART PORTAL’s fire detection devices will activate automatically and notify Simplex Grinnell personnel, who will in turn call Golding Living’s security team, and the fire department in the event of a fire. Westfield provides the space for all information systems in the data center. However, the SMART PORTAL does not employ a fire suppression device within the data center (e.g., FM200). | FAIL | SMART PORTAL |  |
| PE | 14 | 1 | Determine if:   (i) the organization defines the acceptable temperature and humidity levels within the facility where the information system resides;   (ii) the organization maintains temperature and humidity levels within the facility where the information system resides in accordance with organization-defined acceptable levels;   (iii) the organization defines the frequency to monitor temperature and humidity levels;   (iv) the organization monitors the temperature and humidity levels within the facility where the information system resides in accordance with the organization-defined frequency.   (v) the organization meets all the requirements specified below:  a. Evaluate the level of alert and follow prescribed guidelines for that alert level.  b. Alert component management of possible loss of service and/or media.  c. Report damage and provide remedial action. Implement contingency plan, if necessary. | The security guards monitor and record the temperature and humidity levels every hour. In addition, the temperature and humidity are monitored by a Liebert system. When the temperature and humidity exceeds the defined limit, Westfield staff members receive instant notification via text. The ISSO and alternate are notified by telephone when the SMART PORTAL's information system is affected. | PASS | SMART PORTAL |  |
| PE | 15 | 1 | Determine if:   (i) the organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible and working properly;   (ii) key personnel within the organization have knowledge of the master water shutoff values. | The SMART PORTAL has not installed a water shutoff valve that is dedicated to the data center. | FAIL | SMART PORTAL |  |
| PE | 16 | 1 | Determine if:   (i) the organization authorizes, monitors, and controls organization-defined information system components entering and exiting the facility;   (ii) the organization maintains records of information system components entering and exiting the facility. | The SMART PORTAL uses Remedy to document all devices, components and/or system equipment entering and exiting the SMART PORTAL. These changes are reflected in the HHS-565 inventory report generated by Remedy on an annual basis. | PASS | SMART PORTAL |  |
| PE | 17 | 1 | Determine if:   (i) the organization defines the management, operational, and technical information system security controls to be employed at alternate work sites;   (ii) the organization employs organization-defined management, operational, and technical information system security controls at alternate work sites;   (iii) the organization assesses, as feasible, the effectiveness of security controls at alternate work sites;   (iv) the organization provides a means for employees to communicate with information security personnel in case of security incidents or problems. | There are no telework employees in the SMART PORTAL; however in the event telework is permitted the SMART PORTAL would need to create a formal document outlining the detailed security guidelines for an individual's "teleworking" environment. | N/A | SMART PORTAL |  |
| PE | 18 | 1 | Determine if:   (i) the organization positions information system components within the facility to minimize potential damage from physical and environmental hazards;   (ii) the organization positions information system components within the facility to minimize the opportunity for unauthorized access. | All mission critical information systems are located in the AR1-SMART PORTAL Data Center that has been strategically positioned in the facility to minimize the impact of potential environmental hazards. | PASS | SMART PORTAL |  |
| PL | 1 | 1 | Determine if:   (i) the organization develops and formally documents security planning policy;   (ii) the organization security planning policy addresses:  a. purpose;  b. scope;  c. roles and responsibilities;  d. management commitment;  e. coordination among organizational entities;  f. compliance;   (iii) the organization disseminates formal documented security planning policy to elements within the organization having associated security planning roles and responsibilities;   (iv) the organization develops and formally documents security planning procedures;   (v) the organization security planning procedures facilitate implementation of the security planning policy and associated security planning controls;   (vi) the organization disseminates formal documented security planning procedures to elements within the organization having associated security planning roles and responsibilities;   (vii) the organization reviews/updates the security planning policy and procedures within every three hundred sixty-five (365) days. | The SMART PORTAL-SSP version. 3.3 dated April 3, 2013 details the necessary controls required to maintain the security posture of the SMART PORTAL. The SSP is maintained by the ISSO who is responsible for updating and reviewing the SSP on an annual basis. The SMART PORTAL's SSP is disseminated to all personnel with security duties. | PASS | SMART PORTAL |  |
| PL | 2 | 1 | Determine if:   (i) the organization develops a security plan for the information system that:  a. is consistent with the SMART THINK System Security Plan (SSP) Procedure;  b. is consistent with the organization's enterprise architecture;  c. explicitly defines the authorization boundary for the system;  d. describes the operational context of the information system in terms of missions and business processes;  e. provides the security category and impact level of the information system including supporting rationale;  f. describes the operational environment for the information system;  g. describes relationships with or connections to other information systems;  h. provides an overview of the security requirements for the system;  i. describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and  j. is reviewed and approved by the authorizing official or designated representative prior to plan implementation;   (ii) the organization reviews the security plan for the information system within every three hundred sixty-five (365) days;   (iii) the organization updates the plan, minimally every three (3) years, to address current conditions or whenever:  a. there are significant changes to the information system/environment of operation that affect security;  b. problems are identified during plan implementation or security control assessments:  c. when the data sensitivity level increases;  d. after a serious security violation due to changes in the threat environment; or before the previous security authorization expires;   (iv) the System Security Plan is consistent with the organization's information system architecture and information security architecture.   (v) the organization meets all the requirements specified below:  a. (For PHI only) Retain documentation of policies and procedures' relating to HIPAA 164.306 for six (6) years from the date of its creation or the date when it last was in effect, whichever is later. (See HIPAA 164.316(b).)  b. (For FTI only) When FTI is incorporated into a Data Warehouse, the controls described in IRS Pub. 1075, Exhibit 7 are to be followed, in addition to those specified in other controls.  c. (For FTI only) Develop and submit a Safeguard Procedures Report (SPR) that describes the procedures established and used by the organization for ensuring the confidentiality of the information received from the IRS. Annually thereafter, the organization must file a Safeguard Activity Report (SAR). The SAR advises the IRS of minor changes to the procedures or safeguards described in the SPR. It also advises the IRS of future actions that will affect the organization's safeguard procedures, summarizes the organization's current efforts to ensure the confidentiality of FTI, and finally, certifies that the organization is protecting FTI pursuant to IRC Section 6103(p)(4) and the organization's own security requirements. Whenever significant changes occur in the safeguard program the SPR will be updated and resubmitted. (See IRS Pub. 1075, sections 7 & 8) | The SMART PORTAL SSP did not define all security controls that are within the scope and boundary of local SMART PORTAL operations. The following list identifies the security controls that are not included within the SMART PORTAL SSP and currently are incomplete, inaccurate or have been omitted:    • AC-19-Access Control for Portable and Mobile Devices    • PS-2-Position Categorization    • PS-5- Personnel Transfer.  In addition, the SSP does not define the authorization boundary or the security category of the system. | FAIL | SMART PORTAL |  |
| PL | 4 | 1 | Determine if:   (i) the organization establishes the rules that describe information system user responsibilities and expected behavior with regard to information and information system usage;   (ii) the organization makes the rules available to all information system users;   (ii) the organization receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system. | The SMART PORTAL has established a set of rules of behavior (ROB) / code of ethics for all personnel prior to them gaining access to the information system. The SMART PORTAL receives a signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before granting authorized access to the information system. All users are required to complete security awareness training upon initial hire and annually. | PASS | SMART PORTAL |  |
| PL | 6 | 1 | Determine if the organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals. | Appropriate planning and coordination occurs between the SMART PORTAL, SMART THINK, and SMART THINK. Key personnel are informed about on-going security activities through the security awareness training, SMART PORTAL memos, Remedy tickets submitted to the SMART PORTAL and the Smart Portal conference that is held annually. | PASS | SMART PORTAL |  |
| PS | 1 | 1 | Determine if:   (i) the organization develops and formally documents personnel security policy;   (ii) the organization personnel security policy addresses:  a. purpose;  b. scope;  c. roles and responsibilities;  d. management commitment;  e. coordination among organizational entities;  f. compliance;   (iii) the organization disseminates formal documented personnel security policy to elements within the organization having associated personnel security roles and responsibilities;   (iv) the organization develops and formally documents personnel security procedures;   (v) the organization personnel security procedures facilitate implementation of the personnel security policy and associated personnel security controls;   (vi) the organization disseminates formal documented personnel security procedures to elements within the organization having associated personnel security roles and responsibilities;   (vii) the organization reviews/updates the personnel security policy and procedures within every three hundred sixty-five (365) days. | The SMART PORTAL's personnel security procedures are developed and documented within the Arkansas Foundation For Medical Care Employee Handbook dated March 2013 and the AFMC SSP version 3.3 dated April 2013 .The SSP and the Employee Handbook are updated/reviewed annually, as required. | PASS | SMART PORTAL |  |
| PS | 2 | 1 | Determine if:   (i) the organization assigns a risk designations to all positions within the organization;   (ii) the organization establishes a screening criteria for individuals filling organizational positions;   (iii) the organization defines in the System Security Plan, explicitly or by reference, the frequency of risk designation reviews and updates for organizational positions;   (iv) the organization reviews and revises position risk designations within every three hundred sixty-five (365) days. | The SMART PORTAL does not define within the SSP the criteria for arriving at each risk designation. In addition, the SSP must outline the frequency of risk designation reviews and updates.  Risk level designations are not defined for and assigned to all personnel positions and reviewed on an annual basis. In addition, background screening criteria commensurate with the assigned risk levels is not detailed. | FAIL | SMART PORTAL |  |
| PS | 3 | 1 | Determine if:   (i) the organization screens individuals prior to authorizing access to the information system;   (ii) the organization rescreens individuals periodically, consistent with the criticality/sensitivity rating of the position;   (iii) the organization requires that when an employee moves from one position to another, the higher level of clearance should be adjudicated.   (iv) the organization meets all the requirements specified below:  a. Require that individuals with significant security responsibilities be assigned and hold, at a minimum, a Level 5 Public Trust sensitivity level clearance as defined in the HHS Personnel Security/Suitability Handbook. Assign other individuals with Public Trust positions the appropriate sensitivity level as defined in the HHS Personnel Security/Suitability Handbook. | Risk level designations are not defined for and assigned to all personnel positions and reviewed on an annual basis. In addition, background screening criteria commensurate with the assigned risk levels is not detailed. | FAIL | SMART PORTAL |  |
| PS | 4 | 1 | Determine if:   (i) the organization terminates information system access upon termination of individual employment;   (ii) the organization conducts exit interviews of terminated personnel;   (iii) the organization retrieves all security-related SMART THINK information system-related property from terminated personnel;   (iv) the organization, upon termination of individual employment, retrieves all security-related SMART THINK information system-related property;   (v) the organization, upon termination of individual employment, retains access to SMART THINK information and information systems formerly controlled by terminated individual;   (vi) the organization, upon termination of individual employment, immediately escorts employees terminated for cause out of the organization.   (vii) the organization meets the requirement(s) specified below:  a. System access must be revoked prior to or during the employee termination process. | The SMART PORTAL utilizes termination procedures and a termination checklist for all employees that are either being terminated for cause or for voluntary resignation. The ISSO is notified of any resignation of an employee so that access to the building and the information systems is revoked at the end of their last day. For employees terminated for cause, they are escorted off the premises and their computer access is revoked during their exit interview with HR. In either case, all company property is retrieved from the employee (i.e. laptops, building passes, and badges) before they leave the premises. | PASS | SMART PORTAL |  |
| PS | 5 | 1 | Determine if:   (i) the organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization;   (ii) the organization defines the transfer or reassignment actions and the time period within which the actions must occur following formal transfer or reassignment;   (iii) the organization initiates the organization-defined transfer or reassignment actions within an organization-defined time period following formal transfer or reassignment. | Logical and physical access is reviewed by utilizing an Employee Action Form and a Promotion/Transfer Checklist. The hiring manager usually completes the Employee Action Form for transfers and reassignments. However, the transfer procedures and the time period within which the procedures must occur following a transfer is not defined in the HR Manual. | FAIL | SMART PORTAL |  |
| PS | 6 | 1 | Determine if:   (i) the organization identifies appropriate access agreements for individuals requiring access to SMART THINK information and information systems;   (ii) individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access;   (iii) the organization defines in the security plan, explicitly or by reference, the frequency of reviews/updates for access agreements;   (iv) the organization reviews/updates the access agreements as part of the system security authorization or when a contract is renewed or extended, but minimally within every three hundred sixty-five (365) days, whichever occurs first. | The SMART PORTAL has established a set of Rules of Behavior and Code of Conduct for all personnel prior to receiving access to the system. The SMART PORTAL receives a signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system. In addition, all personnel with access to the information system must complete the Security Awareness Training annually. | PASS | SMART PORTAL |  |
| PS | 7 | 1 | Determine if:   (i) the organization establishes personnel security requirements, including security roles and responsibilities, for third-party providers;   (ii) the organization documents personnel security requirements for third-party providers;   (iii) the organization monitors third-party provider compliance with personnel security requirements.   (iv) the organization meets the requirement(s) specified below:  a. Regulate the access provided to contractors and define security requirements for contractors. Contractors must be provided with minimal system and physical access, and must agree to and support the SMART THINK information security requirements. The contractor selection process must assess the contractor's ability to adhere to and support SMART THINK' information security policies and standards. | All third-party providers are treated as visitors. They are required to enter through the main facility access point, show appropriate government issued photo identification, sign the visitor's log and receive a badge that must be worn during their visit. | PASS | SMART PORTAL |  |
| PS | 8 | 1 | Determine if the organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures. | The SMART PORTAL has a progressive disciplinary process in place with actions that include verbal reprimands, written warnings, suspension, or final termination. | PASS | SMART PORTAL |  |
| RA | 1 | 1 | Determine if:   (i) the organization develops and formally documents risk assessment policy;   (ii) the organization risk assessment policy addresses:  a. purpose;  b. scope;  c. roles and responsibilities;  d. management commitment;  e. coordination among organizational entities;  f. compliance;   (iii) the organization disseminates formal documented risk assessment policy to elements within the organization having associated risk assessment roles and responsibilities;   (iv) the organization develops and formally documents risk assessment procedures;   (v) the organization risk assessment procedures facilitate implementation of the risk assessment policy and associated risk assessment controls;   (vi) the organization disseminates formal documented risk assessment procedures to elements within the organization having associated risk assessment roles and responsibilities;   (vii) the organization reviews/updates the risk assessment policy and procedures within every three hundred sixty-five (365) days. | The SMARTPORTAL has not developed a formal risk assessment plan for the facility. | FAIL | SMART PORTAL |  |
| RA | 3 | 1 | Determine if:   (i) the organization conducts an assessment of risk of the information system and the information it processes, stores, or transmits that includes the likelihood and magnitude of harm, from the unauthorized:  a. access;  b. use;  c. disclosure;  d. disruption;  e. modification; or  f. destruction;   (ii) the organization documents risk assessment results in accordance with the SMART THINK IS RA Procedures;   (iii) the organization reviews risk assessment results within every three hundred sixty-five (365) days;   (iv) the organization updates the risk assessment within every three (3) years or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security or authorization state of the system. | The SMART PORTAL has not developed a formal risk assessment plan for the facility. | FAIL | SMART PORTAL |  |
| SA | 3 | 1 | Determine if:   (i) the organization manages the information system using the information security steps of IEEE 12207.0 standard for SDLC, as provided in the SMART THINK Integrated IT Investment & System Life Cycle Framework (ILC);   (ii) the organization defines and documents information system security roles and responsibilities throughout the system development life cycle;   (iii) the organization identifies individuals having information system security roles and responsibilities. | The SMART PORTAL manages Smart Portal using the SMART THINK eXpedited Life Cycle (XLC) methodology which incorporates information security considerations. The SMART PORTAL security roles and responsibilities are documented in the Smart Portal System Security Policy, version 7.0, dated July 2011 as well as the SMART PORTAL SSP. | PASS | SMART THINK SMART PORTAL | Project Plan implementing the system development life cycle methodology, Systems Development Life-Cycle Methodology and Guidance documents |
| SA | 4 | E1 | Determine if the organization requires in acquisition that vendors/contractors provide information describing the functional properties of the security controls to be employed within the information system, information system components, or information system services in sufficient detail to permit analysis and testing of the controls. | SMART THINK usually handles purchasing SMART PORTAL equipment that requires them to compile the necessary specifications and/or features from SMART THINK and the SMART PORTAL community at large. Each request must undergo the Engineering Review Board (ERB) process so that a full evaluation can be conducted to ensure that the requested item meets the security requirements of SMART THINK guidance. | PASS | SMART THINK SMART PORTAL |  |
| SC | 9 | 1 | Determine if:   (i) the information system protects the confidentiality of transmitted information.   (ii) the organization meets all the requirements specified below:  a. (For PII only) When sending or receiving faxes containing PII: (i) fax machines must be located in a locked room with a trusted staff member having custodial coverage over outgoing and incoming transmissions or fax machines must be located in a secured area; (ii) accurate broadcast lists and other preset numbers of frequent fax recipients must be maintained; and (iii) a cover sheet must be used that explicitly provides guidance to the recipient that includes: a notification of the sensitivity of the data and the need for protection, and a notice to unintended recipients to telephone the sender (collect if necessary) to report the disclosure and confirm destruction of the information. | All protection measures including the Smart Portal exchange application, Pointsec Media Encryption software and secured fax areas are in place to protect all transmission of sensitive information (PII/PHI). | PASS | SMART PORTAL |  |
| SC | 15 | 1 | Determine if:   (i) the organization prohibits running collaborative computing mechanisms, unless explicitly authorized, in writing, by the CIO or his/her designated representative;   (ii) if authorized, the authorization shall specifically identify allowed mechanisms, allowed purpose, and the information system upon which the mechanisms can be used;   (iii) if authorized, the information system prohibits remote activation of collaborative computing devices;   (iv) if authorized, the information system provides an explicit indication of use to users physically present at the devices. | The SMART PORTAL does not use any collaborative computing equipment. | N/A | SMART PORTAL |  |
| SC | 15 | E1 | Determine if the information system provides physical disconnect of collaborative computing devices in a manner that supports ease of use. | Video teleconference is not used at the SMART PORTAL. | N/A | SMART PORTAL |  |
| SC | 19 | 1 | Examine/Interview if:   (i) the organization establishes usage restrictions and implementation guidance for Voice over Internet Protocol technologies based on the potential to cause damage to the information system if used maliciously.   (ii) the organization authorizes, monitors, and controls the use of VoIP within the information system. | VoIP is not employed at the SMART PORTAL. | N/A | SMART THINK SMART PORTAL |  |
| SI | 12 | 1 | Determine if:   (i) the organization handles both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements;   (ii) the organization retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.   (iii) the organization meets all the requirements specified below:  a. Retain output, including, but not limited to audit records, system reports, business and financial reports, and business records, from the information system in accordance with SMART THINK Policy and all applicable National Archives and Records Administration (NARA) requirements. | The SMART PORTAL adheres to the necessary requirements for output handling and retention (i.e. sensitive documentation such as PII) in accordance with applicable regulations and SMART THINK Policy. | PASS | SMART PORTAL |  |

**End of Document**