Restricted Distribution
Sensitive Information – For Official Use Only

Centers for Medicare & Medicaid Services

ACA System Security Plan Procedures

Version 1.0

August 1, 2012

Table of Contents

INTRODUCTION

The Centers for Medicare & Medicaid Services (CMS) is responsible for implementing many provisions of the historic health insurance reform law called the Affordable Health Care Act (ACA). The Center for Consumer Information and Insurance Oversight (CCIIO), a new group in CMS, is responsible for facilitating the implementation of these programs and initiatives. These initiatives will benefit millions of Americans in obtaining affordable health care services and also enabling more employers to offer insurance coverage in a cost effective manner to their employees.

The ACA provides for each state to have a health insurance Exchange. An Exchange is an organized marketplace to help consumers and small businesses to buy health insurance in a way that permits easy comparison of available plan options based on price, benefits and services, and quality. Consumers seeking health care coverage will be able to go to the health insurance Exchanges to obtain comprehensive information on coverage options currently available and make informed health insurance choices. By pooling consumers, reducing transaction costs, and increasing transparency, Exchanges create more efficient and competitive health insurance markets for individuals and small employers.

CMS is responsible for providing guidance and oversight for the Exchanges and for state IT systems that facilitate common electronic enrollment. This responsibility includes defining business, information, and technical guidance that will create a common baseline and standards for these IT system implementation activities.

1.1 OVERVIEW

Protecting and ensuring the confidentiality, integrity, and availability (CIA) for state Exchange and common enrollment information and information systems is the responsibility of the states; the Affordable Care Act charges CMS with responsibility for oversight of the Exchange and common enrollment IT systems.

The Health and Human Services Final Rule on Exchange Establishment also requires exchange systems processing of Federal Tax Information (FTI), as defined in section 6103(b)(2) of the Code, be kept confidential and disclosed, used, and maintained only in accordance with section 6103 of the Code.

The *System Security Plan (SSP)* and the *Safeguard Procedures Report (SPR)* together document the implementation of the comprehensive control requirements of ACA regulations for the protection of all data received, stored, processed and transmitted by the health insurance exchanges and data services hub. The SSP is comprised of two main sections: the first section, System Identification, highlights overall systems and business design and functionality, while the second section, Security Control Details, provides a detailed description of the implementation

details of each security control. The SSP Workbook, providing a comprehensive description of the security controls common to both CMS and IRS requirements, is to be used for supplying the information in the Security Control Details section. Security controls specific to the protection of FTI or requirements above the common control baseline must be documented in the SPR. Together, these documents form the description of the controls in place to protect all data contained in health insurance exchange and data services hub systems – both FTI and non-FTI.

1.2 PURPOSE

The primary goal of this procedure is to lay out the minimum requirements to describe the security protections for health insurance exchange systems (either state or federal) and to standardize the work of the System Developer/Maintainers and the Business Owners or equivalents in creating SSPs.

The purpose of the SSP/SSP Workbook/SPR package is to:

- Identify applicable laws and/or regulations affecting the system;
- Identify the rules of behavior associated with the system;
- Identify and provide details on the security controls related to the system within the NIST 800-53, *Recommended Security Controls for Federal Information Systems* (for moderate impact level), control families and those for FTI, if applicable;
- Capture both high and moderate level risks identified during the risk assessment;
- Identify how security is addressed in all levels of development;
- Identify personnel responsible for oversight, development and the security of the system;
- Identify the business process (es) associated with the system;
- Identify the system environment;
- Identify system interconnections; and
- Identify the system security level.

The security controls are organized into *families* for ease of use in the control selection and specification process. There are eighteen (18) security control families from NIST 800-53 and additional safeguards required by IRC § 6103(p) (4) as defined by Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies*, for federal tax information. Each family contains security controls related to the security functionality of the family. Controls common to both CMS and IRS requirements are documented in the SSP Workbook. The agency must fully explain how the control requirement will be implemented. Controls specific to the protection of FTI or controls above the common controls must be documented in the SPR. Table 1, Security Control Classes, Families and Identifiers describes the families and classes of the security controls.

Note: although a control family may cover more than one function, the class most represented

by the control is the designated class.

TABLE 1: SECURITY CONTROL CLASSES, FAMILIES AND IDENTIFIERS

IDENTIFIER	FAMILY	CLASS
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Certification, Accreditation and Security Assessments	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational
PM	Program Management	Management
IRC §6103(p)(4)	Safeguarding federal tax information	FTI
Publication 1075	Safeguarding federal tax information	FTI

1.3 SSP/SPR Template Instructions

The purpose of this section is providing detailed instructions for completing the SSP package, using the SSP template, the SSP Workbook and the SPR.

A completed SSP package must contain technical information about the system, its security requirements and the controls implemented to provide protection against its vulnerabilities. The SSP package will also document the policies, processes and procedures associated with the health insurance exchange (state and federal), both at the program and systems levels. All SSPs must be dated to allow ease of tracking modifications and approvals (every page must have date, version number, page number and total number of pages on it).

Instructions on how to complete the templates have been developed for each section within the template and shall be used for all sensitivity levels.

1.4 EXECUTIVE SUMMARY

An Executive Summary is **OPTIONAL**. If included, provide a summary of each of the first four (4) sections of the SSP. Do not restate procedure; only provide a summary of facts about the

system and business processes being documented. If an executive summary is included with the SSP, it must be no more than one (1) single spaced page in length.

2 SYSTEM IDENTIFICATION

2.1 SYSTEM NAME AND TITLE

Provide the system identifier, which include the official name and/or title of system, including acronym.

2.2 RESPONSIBLE ORGANIZATION

Provide the contact information for the organization responsible for the system. The organization is responsible for coordinating System Development Life Cycle (SDLC) activities specific to the system. The SSP should include the following contact information:

- Name of Organization;
- Address;
- City, State, Zip;
- Contract Number; and
- Contract Name.

2.3 DESIGNATED CONTACTS

Indicate the names of other key contact personnel who can address inquiries regarding system characteristics and operation. Required contacts include, but are not limited to, Business Owner, System Developer/Maintainer, SSP author, (or equivalent), etc. The SSP should include the following contact information for each of the other designated contacts:

- Name:
- Title;
- Organization;
- Address;
- Mail stop;
- City, State, Zip;
- E-mail;
- Telephone; and
- Contractor contact information (if applicable).

Identify any additional personnel that can address system related inquiries. Provide contact information for each.

2.4 ASSIGNMENT OF SECURITY RESPONSBILITY

Identify one (1) primary security contact and one (1) different emergency contact. The emergency contact should know how to contact the primary contact or his/her supervisor. The emergency contact does not have to be a technical person. The assignment of security

responsibility shall include the contacts following information:

- Name;
- Title;
- Organization;
- Address;
- Mail stop;
- City, State, Zip;
- E-mail;
- Telephone number: and
- Emergency Contact

2.5 SYSTEM OPERATIONAL STATUS

Annotate whether the General Support System (GSS) or Major Application (MA) is New, Operational or Undergoing Major Modification.

2.6 DESCRIPTION OF THE BUSINESS PROCESS

Provide a brief description of the system:

- Indicate the location of the system. This high-level description shall include the street address and other information pertaining to the location of the system;
- Describe the business function for each system. Also include information regarding the overall business processes, including any business system diagrams;
- Describe the underlying business processes and resources that support each business function. This may include the required inputs (business functions/processes that feed this function), processing functions (calculations, etc.), organizational/personnel roles and responsibilities, and expected outputs/products (that may "feed" other business functions / processes;
- Describe how information flows through/is processed by the system, beginning with system input through system output. Further describe how the data/information is handled by the system (is the data read, stored, purged, etc.?). Note: a data flow chart and explanation specific to the receipt, processing, storage, transmission and destruction of FTI is required by SPR section 3.1. Generally, the FTI data flow is a subset of the overall data flow;
- Indicate the organizations (internal & external) that will comprise the user community. Include type of data and processing that will be provided by users, if any; and
- Describe the users' level of access to: system-related data (read-only, alter, etc.), system-related facilities, and information technology resources.

2.7 DESCRIPTION OF OPERATIONAL / SYSTEM ENVIRONMENT AND SPECIAL CONSIDERATIONS

2.7.1 Operational Information

Describe (at a high level) the anticipated technical environment and user community necessary to support the system and business functions. Include:

- Communications requirements;
- User-interface expectations; and
- Network connectivity requirements.

Be sure to indicate, the physical location of the business processes and technology that will support the system.

2.7.2 System Information

Provide a brief general description of the technical aspects of the system. Include any environmental or technical factors that raise special security concerns, such as use of Personal Digital Assistants, wireless technology, etc.

Attach the network connectivity diagram, which shall address the system components' connection, and the security devices, which 1) protect the system; and, 2) monitor system access and system activity. For systems that have more than one server of the same type, only include one in the diagram; however state the accurate count of the servers in the supporting text description. Be sure to provide an opening sentence(s) prior to the diagram. Following the diagram, include text that will explain system components and function. Be sure to number system components in the diagrams to correlate with the information presented.

2.7.3 System Environment

Provide a description of the system environment:

- Is the system owned or leased?
- Is the system operated by the State or by a support service contractor? If the system is operated by the state run consolidated data center, provide the name, location and point of contact for the consolidated data center.
- If the system is maintained or "run" by a contractor, describe (comprehensively) how the system is managed.
- Document the hours of operation: e.g. 24x7, M-F 7:30 am – 5:00 pm.
- Document the approximate total number of user accounts and unique user types (i.e. researchers, programmers, administrative support, caseworkers, public-facing employees, etc.).
- Identify the critical processing periods (e.g., eligibility processing.).
- If system serves a large number of off-site users, list both the organizations and types of

users (e.g., other agencies, assistors, navigators).
- List all applications supported by the system including the applications' functions and information processed.
- Describe how system users access the system (i.e., desktop, thin client, etc.). Include any information required to evaluate the security of the access.
- Describe the information / data stores within the system and security controls for such data.
- Describe the purpose and capabilities of the information system. Describe the functional requirements of the information system. For instance:
  - Are protection mechanisms (i.e., firewalls) required?
  - Are support components such as web servers and e-mail required?
  - What types of access mechanisms (i.e., telecommuting, broadband communications) are required?
  - Are "plug-in" methods (Mobile code; Active-X, Javascript) required?
  - What operating system standards, if any, are required?

2.7.4 Architecture and Topology

Describe the architecture of the information system.

- Describe the network connection rules for communicating with external information systems.
- Describe the functional areas within the architecture (presentation, application and data zones, if applicable) and how this addresses security.

2.7.5 System Boundary

Provide a detailed description of the system's boundaries and technical components.

- Describe the boundary of the information system for security accreditation.
- Describe the hardware, software, and system interfaces (internal and external) to include interconnectivity.
- Describe the network topology.
- Include a logical diagram for system components with system boundaries, if needed, to clarify understanding of the system function and integration.
- Following the logical diagram, describe the information flow or processes within the system to access to the data/information.

2.7.6 Primary Platforms and Security Software

Describe the primary computing platform(s) used and describe the principal system components, including hardware, firmware, software, wireless and communications resources. Include any environmental or technical factors that raise special security concerns (dial-up lines, open network, etc.). This will include vendors and versions.

- Include information concerning a system's hardware and platform(s).
- Detailed hardware equipment information, such as server names, shall be listed and attached to the documentation.

- Describe any security software protecting the system and information.
- Describe in general terms the type of security protection provided (e.g., access control to the computing platform and stored files at the operating system level or access to data records within an application). Include only controls that have been implemented, rather than listing the controls that are available in the software.

2.7.7 Interconnectivity Interfaces, Web Protocols and Distributes & Collaborative Computing Environments

Describe the Web protocols and distributed, collaborative computing environments (i.e., processes and applications).

- Describe the connectivity between modules within the scope of this system.
- For any system that allows individual web-based access (Internet, Intranet, Extranet) to conduct transactions the following information should be provided:
  - The Uniform Resource Locator (URL) for the web-based transaction;
  - E-authentication architecture implemented;
  - E-authentication interoperable product used;
  - Other authentication products used;
  - Number of electronic logons per year;
  - Number of registered users (Government to Government);
  - Number of registered users (Government to Business);
  - Number of registered users (Government to Citizen);
  - Number of registered internal users; and
  - Description of customer groups being authenticated, e.g., Business Partners, Medicare Service Providers, Beneficiaries, etc.

2.7.8 Special Security Concerns

Include any environmental or technical factors that raise special security concerns, such as:

- Indicate the physical location of the information system;
- The system is connected to the Internet;
- It is located in a harsh or overseas environment (FTI is not allowed offshore);
- Software is implemented rapidly;
- The software resides on an open network used by the public or with overseas access (FTI is not allowed offshore); and
- The application is processed at a facility outside of State control.

2.8 SYSTEM INTERCONNECTION / INFORMATION SHARING

System interconnection is the direct connection of two or more IT systems for sharing information resources. It is important that Business Owners and management obtain as much information as possible regarding vulnerabilities associated with system interconnections and information sharing. This is essential in selecting the appropriate

controls required to mitigate those vulnerabilities.

A Master Interconnection Security Agreement (ISA) and/or Master Memorandum of Understanding (MOU) is required between States and the Federal Exchange and Data Services Hub, which share data, and are owned or operated by different organizations. Describe the information sharing agreement in place to govern the data exchange. If not yet finalized, provide the current status as well.

2.9 SYSTEM SECURITY LEVEL

Identify the system security level. Assistance in categorizing system security level can be found at the CMS IS website:

http://www.cms.hhs.gov/InformationSecurity/Downloads/ssl.pdf

Describe in general terms the information handled by the system and the protective measures.

2.10 E-AUTHENTICATION ASSURANCE LEVEL

Identify the appropriate box concerning the system/application's ability to provide web-based access to individuals for the purpose of conducting transactions. If web-based transactions are permitted, and RACF/Top Secret/Active Directory (or equivalent) is used to authenticate individuals, provide response data in the appropriate box.

NIST SP 800-63, *Electronic Authentication Guideline*, and the Office of Management and Budget (OMB) Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, provide guidance in establishing the level of e-Authentication security required for systems. The guidance addresses all four (4) levels of assurance for E-authentication.

2.11 APPLICABLE LAWS OR REGULATIONS

List any state laws (state insurance exchanges), regulations, specific standards, guidance or policies governing the creation of ACA-related systems, organizations and business processes.

2.12 RULES OF BEHAVIOR

Indicate the following information but not limited to:

- A definition of each type of user of the system (i.e. user, developer, sys admin, DB admin, etc.) and a summary of the Rules of Behavior (ROB) or "code of conduct" specific to the system for each type of user, including how often the system users are required to re-acknowledge the rules and how this process is documented;
- Password construction / maintenance;
- Changing system data;
- Searching databases;
- Divulging information;
- Working at home;

- Dial-in access;
- Connection to the Internet; and
- Assignment and limitation of system privileges.

The ROB must include the consequences of non-compliance and must clearly state the exact behavior expected of each person.

3 SECURITY CONTROLS DETAIL AND COMMENTS

The SSP Workbook and SPR coupled together provide the comprehensive control requirements that must be documented for the protection of all data received, stored, processed and transmitted by the health insurance exchanges and data services hub for implementation of the ACA legislation. Security controls common to both CMS and IRS requirements are documented in the SSP Workbook. Security controls specific to the protection of FTI or requirements above the common control baseline must be documented in the SPR. Together, the SSP Workbook and SPR form the description of the controls in place to protect all data contained in health insurance exchange and data services hub systems – both FTI and non-FTI.

- Describe how the security controls are implemented for all of the security control families within the SSP Workbook and SPR.
- Discuss in detail the strategy used in implementing the controls.
- Include in the Configuration Management (CM) control section the baseline security configurations of the system/application.
- At the bottom of each control section, document the organizational component or contractor responsible for supporting and maintaining the control.

4 APPENDICES AND ATTACHMENTS

The following appendices represent documentation that may be developed and maintained as separate documents but must be included with the SSP package for evaluation. Maintaining these documents as appendices facilitates configuration management of all the related materials. These appendices should be updated if there is a major change in the security profile. At a minimum, the SSP package must contain the following:

Appendices:

- Appendix A - This appendix contains a listing of equipment that supports the System/Application. This appendix should be labeled as APPENDIX A – EQUIPMENT LIST;
- Appendix B - This appendix contains a listing of software that supports the System/Application. This appendix should be labeled as APPENDIX B – SOFTWARE LIST;

- Appendix C – This appendix contains the detailed configuration settings that satisfy the required CMS baseline configurations. This appendix should be labeled as APPENDIX C – DETAILED CONFIGURATION SETTINGS;
- Appendix D – This appendix contains the glossary of terms used in the SSP and is provided for additional clarity This appendix should be labeled as APPENDIX D – GLOSSARY; and
- Appendix E – This appendix contains the acronyms and abbreviations used in the SSP and are provided for additional clarity. This appendix should be labeled as APPENDIX E – ACRONYMS AND ABBREVIATIONS.

Attachments:

- Attachment 1 - SYSTEM SECURITY PLAN WORKBOOK

  Controls common to both CMS and IRS requirements are documented in the SSP Workbook. The agency must fully explain how the control or requirement will be implemented.
- Attachment 2 - IRS SAFEGUARD PROCEDURES REPORT (SPR)
  Controls specific to the protection of federal tax information (FTI) or requirements above the common controls must be documented in the SPR. Together, the SSP and SPR form the description of all data – both FTI and non-FTI.