The table below capture changes when updating the document. All columns are mandatory.

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Date</th>
<th>Chapter Section</th>
<th>Author/Owner Name</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>01/31/2017</td>
<td>All</td>
<td>CMS ISPG</td>
<td>DRAFT initial version</td>
</tr>
<tr>
<td>2.1</td>
<td>03/17/2021</td>
<td>3.1.4 System Security Plan Approval</td>
<td>CMS ISPG</td>
<td>Incorporated language to submit ATO Memo to FedRAMP PMO upon approval</td>
</tr>
</tbody>
</table>
Effective Date/Approval

This Procedure becomes effective on the date that CMS’s Director, Division of Security and Privacy Policy and Governance (DSPPG) signs it and remains in effect until it is rescinded, modified or superseded.

Signature: /S/  Date of Issuance _________

Michael Pagels
Director, Division of Security and Privacy Policy and Governance (DSPPG) and Acting Senior Official for Privacy
Table of Contents

Record of Changes.......................................................................................................................... ii
Effective Date/Approval.................................................................................................................. iii
Table of Contents........................................................................................................................ iv

1. Executive Summary .................................................................................................................. 5
2. Common Control Inheritance.................................................................................................. 5
3. Procedures ................................................................................................................................. 6
   3.1 System Security Plan (PL-2) .............................................................................................. 6
   3.1.1 Security Categorization................................................................................................. 7
   3.1.2 Security Control Selection........................................................................................... 9
   3.1.3 Documenting Security Control Implementations ..................................................... 11
   3.1.4 System Security Plan Approval.................................................................................. 13
   3.1.5 System Security Plan Update and Maintenance .................................................... 15
   3.1.6 Plan/Coordinate with Other Organizational Entities (PL-2(3)) .............................. 16
   3.2 Rules of Behavior (PL-4) ................................................................................................. 17
   3.2.1 Social Media and Networking Restrictions (PL-4(1)) ............................................. 18
   3.3 Information Security Architecture (PL-8) ...................................................................... 18

Tables

Table 1: Common Control Inheritance ....................................................................................... 5
Table 2: CMS Defined Parameters – Control PL-2 ................................................................. 6
Table 3: CMS Defined Parameters – Control PL-2(3) ............................................................ 16
Table 4: CMS Defined Parameters – Control PL-4 ................................................................ 17
Table 5: CMS Defined Parameters – Control PL-8 ................................................................. 18
1. Executive Summary

RMH Chapter 12 Security and Privacy Planning (PL) is the first handbook that CMS Stakeholders should reference when beginning a new Authorized to Operate (ATO) cycle (new or reauthorization). This chapter not only helps to address the PL control family, but also assists in the overall planning and documentation of key elements needed to obtain an ATO. The controls listed in this section focus on how the organization must develop, document, periodically update, and implement the System Security Plan (SSP) for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems. This chapter also addresses the information security architecture of the information system.

2. Common Control Inheritance

The inherited controls list can be used to identify common controls offered by system alternatives. The use of inherited controls is optional, the objective of this processes is to identify opportunities to extract benefits (and reduce costs) by maximizing the use of already existing solutions, and minimizing duplication of efforts across the enterprise. Below is a listing of controls that can be inherited, where they can be inherited from and if they are a hybrid control for this control family.

<table>
<thead>
<tr>
<th>Planning and Security Control</th>
<th>Inheritable From</th>
<th>Hybrid Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>PL-01</td>
<td>OCISO Inheritable Controls</td>
<td>Yes</td>
</tr>
<tr>
<td>PL-02</td>
<td>CMS Baltimore Data Center - EDC4</td>
<td>No</td>
</tr>
<tr>
<td>PL-02(3)</td>
<td>CMS Baltimore Data Center - EDC4</td>
<td>No</td>
</tr>
<tr>
<td>PL-04</td>
<td>OCISO Inheritable Controls</td>
<td>Yes</td>
</tr>
<tr>
<td>PL-04(01)</td>
<td>CMS Baltimore Data Center - EDC4</td>
<td>No</td>
</tr>
<tr>
<td>PL-08</td>
<td>CMS Baltimore Data Center - EDC4</td>
<td>No</td>
</tr>
</tbody>
</table>
3. Procedures

Procedures assist in the implementation of the required security and privacy controls.

In this section, the PL family procedures are outlined. To increase traceability, this procedure maps to the associated National Institute of Standards and Technology (NIST) security controls using the corresponding control number from the CMS Information Systems Security and Privacy Policy (IS2P2).

3.1 System Security Plan (PL-2)

The purpose of a SSP is to provide an overview of the security requirements of a system and describe the controls that are in place or planned to meet those requirements. The SSP also outlines responsibilities and expected behavior of all individuals who access the system. Creation of the SSP represents a structured process of planning adequate and cost-effective security protection for a system.

The table below outlines the CMS organizationally defined parameters (ODPs) for PL-2.

<table>
<thead>
<tr>
<th>Control</th>
<th>Control Requirement</th>
<th>CMS Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>PL-2</td>
<td>The organization:</td>
<td>The organization:</td>
</tr>
<tr>
<td></td>
<td>b. Distributes copies of the security plan and communicates subsequent changes to the plan to [Assignment: organization-defined personnel or roles];</td>
<td>b. Distributes copies of the security plan and communicates subsequent changes to the plan to stakeholders. The Stakeholders include:</td>
</tr>
<tr>
<td></td>
<td>c. Reviews the security plan for the information system [Assignment: organization-defined frequency];</td>
<td>System Developer and Maintainer (SDM)/Administrators</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Business Owner (BO)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Chief Information Officer (CIO)/Authorizing Official (AO)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cyber Risk Adviser (CRA)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Information System Owner (ISO)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Information System Security Officer (ISSO)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Senior Official for Privacy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Contingency Personnel</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Incident Response Personnel</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Privacy Advisor</td>
</tr>
<tr>
<td></td>
<td>c. Reviews the security plan for the information system within every three hundred sixty-five (365) days;</td>
<td>c. Reviews the security plan for the information system within every three hundred sixty-five (365) days;</td>
</tr>
</tbody>
</table>

At CMS, a SSP is a single document generated by the CMS Federal Information Security Modernization Act Controls Tracking System (CFACTS). A CFACTS generated SSP relates the
CMS security requirements defined in the CMS IS2P2 to a set of security controls and control enhancements as outlined in the CMS Acceptable Risk Safeguards (ARS).

In order to ensure the SSP reflects adequate protection of the information resources, a senior management official must authorize a system to operate. The authorization of a system is granted by an AO and is an important quality control. By authorizing the processing of a system, the AO accepts its associated risk. Authorization should be based on an assessment of management, operational, and technical controls. Since the SSP establishes and documents the security controls, it should form the basis for the authorization, supplemented by the Security Assessment Report (SAR), Certification Form, and the Plan of Actions and Milestones (POA&M).

All CMS information systems must develop and maintain a SSP, which must be compliant with current CMS guidelines, consistent with the CMS Technical Reference Architecture (TRA), and tracked by the CMS CFACTS tool. SSP development should begin for an information system during the Initiation, Concept, and Planning phase of the CMS System Development Life Cycle (CMS-SDLC)\(^1\) as this will ensure that security controls are integrated during the development of the system.

The following sub-section contains the detailed procedures describing how to complete the various sections of the SSP using the CMS CFACTS tool\(^2\).

### 3.1.1 Security Categorization

Each new system must define its security categorization within CFACTS. Before the system security plan can be developed, the information system and the information resident within that system must be categorized based on the Federal Information Processing Standards Publication 199 (FIPS 199)\(^3\). NIST Special Publication 800-60 Revision 1 Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories\(^4\) provides a guideline for mapping types of information and information systems to security categories and was written to work in conjunction with FIPS 199. CMS currently utilizes eleven of the data types listed in NIST Special Publication 800-60 and has configured the CFACTS tool to only display these data types. Authorization boundaries\(^5\) are also developed and reviewed in correlation with the security categorization as the boundary has a direct effect on the categorization of the system. The security categorization for an information system is completed by the ISSO and approved by the Information System Owner.

The following steps detail the CMS specific process for conducting a security categorization on an information system using CFACTS:

---

\(^1\) The CMS SDLC is currently the CMS Target Life Cycle (TLC).

\(^2\) The CFACTS User Manual contains more information on the various sections of the SSP and it would need to be constantly updated in order to be consistent with the latest version of the published User Manual, which is currently CFACTS User Manual V4.5 (11/15/2019). The manual is located on the Homepage of CFACTS, under ‘CFACTS Documents’ [https://cfacts3.cms.cmsnet/apps/ArcherApp/Home.aspx](https://cfacts3.cms.cmsnet/apps/ArcherApp/Home.aspx)


\(^4\) For more information on information type and NIST 800-60 Volume I go to [http://nvlpubs.nist.gov/nistpubs/SP/nistspecialpublication800-60v1r1.pdf](http://nvlpubs.nist.gov/nistpubs/SP/nistspecialpublication800-60v1r1.pdf)

\(^5\) Section 4.4.1 of the CFACTS User Manual contains more information on authorization boundaries.
• **Step 1:** Login to CFACTS and select the “Assessment & Authorization (A&A)” tab from the top menu

• **Step 2:** Expand “Authorization Package” from the downward point triangle icon:

This will expand the menu options and now appear as:

![Assessment & Authorization (A&A)](image)

• **Step 3:** Click on “Authorization Package -Records” in the “Quick Links” list and look for the appropriate information system from the generated report by searching the available Authorization Package records generated

• **Step 4:** Once the information system has been located on the “Information System Name or Program Name” column, click on the hyperlink that corresponds to your Authorization Package system name in order to open the authorization package for the system

• **Step 5:** Select the “Security Category” tab from the top navigation tab of the authorization package

• **Step 6:** Click “Edit” at the top of the authorization package window

• **Step 7:** Answer the following question in the Organizational Users Section “Is this system accessed by non-organizational users?”
  - For help determining who is considered an organizational user and a non-organizational user, see the help text by clicking on the question mark to the left of the question

• **Step 8:** Select the information types processed, stored or transmitted by the system:
  - In the Information Type section click on the right hand side of the “Lookup” title bar in the upper right hand corner
  - In the “Record Lookup” pop up select the checkbox to the left of each information type that is used by your information system
  - Click “Ok” when done

• **Step 9:** Click the “Save” at the top of the screen to save all changes and commit the record(s) to CFACTS
3.1.2 Security Control Selection

For each information system, the appropriate baseline of security controls is automatically allocated by CFACTS based on the information system’s defined security category. For this reason, the security category must be completed for the information system prior to tailoring the security controls. Refer to section 3.1.1 above for the procedures to complete the security categorization.

For control allocation and tailoring, CFACTS implements the following characterizations of security controls:

- **Common Controls:** Common Controls are security controls whose implementation results in a security capability that is inheritable by one or more organizational information systems. Security controls are deemed inheritable by information systems or information system components when the systems or components receive protection from the implemented controls but the controls are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the systems or components—entities internal or external to the organizations where the systems or components reside. However at CMS, a common control isn’t always inherited. Not all applications in CFACTS have a system to inherit from, i.e., ServiceNow (since the ServiceNow Data Center has not been added to CFACTS, it cannot be inherited from.)

- **Cloud Service Providers (CSP) Controls:** The high level process for identifying CSP controls that are inheritable in CMS are as follows:
  - Systems controls are allocated to the system based upon the FIPS 199 security category which is calculated based upon a couple of CFACTS questions. Refer to section 3.1.1 for the steps on conducting a security categorization on an information system using CFACTS.
  - The ISSO needs to walk through each of the controls and determine whose responsibility it is for each control. Outside CFACTS, meetings with the Datacenter/CSP should determine what controls the Datacenter/CSP will be responsible for and what, if anything, the inheriting system needs to do to properly inherit those controls. Most inherited controls require work on the part of the inheriting system.
  - If the datacenter/CSP is responsible, then the ISSO selects the allocation type and also selects the appropriate Datacenter/CSP in the Control Details section.
  - The ISSO repeats this process for each control.

- **Hybrid Controls:** Hybrid Controls are security or privacy controls that are implemented in an information system in part as a common control and in part as a system-specific control.

---

6 Section 4.5.4 of the CFACTS User Manual contains more information on security control allocation.
7 For more information on common controls go to [https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf)
• **System Specific Controls:** System Specific Controls are security controls for an information system that have not been designated as a common security control or the portion of a hybrid control that has to be implemented within an information system. System-specific controls are the primary responsibility of information system owners.

• **Allocated Controls:** In CFACTS, Allocated Controls are those controls attributed/assigned to the information system.

It is possible in CFACTS to tailor the initial baseline of security controls. Tailoring activities consist of adding additional controls for extra security based on an assessment of risk, identifying controls that are not applicable using scoping guidance, and by applying common and hybrid controls. Once tailoring activities have been completed, the tailored set of security controls provides an overview of the security requirements for the system.

The following steps detail the CMS specific process for allocating and tailoring the initial baseline of security control in CFACTS:

- **Step 1:** Login to CFACTS and select the “Assessment & Authorization (A&A)” tab from the top menu.
- **Step 2:** Expand “Authorization Package” from the downward point triangle icon.
- **Step 3:** Click on “Authorization Package -Records” in the “Quick Links” list and look for the appropriate information system from the generated report by searching the available Authorization Package records generated.
- **Step 4:** Once the information system has been located, click on the system name to open the authorization package for the system.
- **Step 5:** Select the “Controls” tab from the top menu of the authorization package.
- **Step 6:** Under the “Allocate Baseline Controls” section, in edit mode, click the radio button labeled “Ready to Allocate.” When this radio button is selected a button labeled “Allocate Controls” will appear on the right side of the section. Click this button to allocate the initial baseline of security controls. It is important to note that prior to allocating baseline security controls to an information system the “Security Category” tab and the “Boundary” tab must be completed. After the clicking the “Allocate Controls” button the process will take several minutes to complete and the screen will need to be refreshed before the security controls will show up in a list under the “Allocated Controls” section. It is a good idea to Save and close the record at this point. The user can open the record and the Controls tab again once they have waited long enough for the internal process to create the controls list for this Authorization Package.
- **Step 7:** To tailor a security control identify the control from the list of allocated controls and click on the control number.

---

8 Section 4.4 of the CFACTS User Manual contains more information on the Boundary tab.
• **Step 8:** Under the “Allocated Controls” box click the “Edit” button in the upper left hand corner

• **Step 9:** Scroll down to the “Control Allocation” section and select “Inherited” to apply a common control or “Not Applicable” if the control does not apply to the information system. If a status of “Not Applicable” is selected, then a “Reason for De-allocation” dialogue box will appear to the right. This field must be completed and should contain an explanation of why the control is not required for the information system. If a status of “Inherited” is selected, then the user must complete the “Control to Inherit” section by clicking the “Lookup” link in the upper right hand corner of that section and selecting the security control and authorization package providing the control from the list

• **Step 10:** Click “Save” to apply the tailoring for that control and return to the list of allocated controls

• **Step 11:** To add a control that was not allocated as a result of the initial allocation described above in Step 6, if the user wishes to add a control that CFACTS did not allocate, the user will have to make a request to have that control added to the system Authorization Package

• **Step 12:** Under the “Allocated Controls” box click the “Edit” button in the upper left hand corner

• **Step 13:** Scroll down to the “Control Allocation” section and select “Allocated”

• **Step 14:** Click “Save” to apply the tailoring for that control and return to the list of allocated controls

### 3.1.3 Documenting Security Control Implementations

All Business Owners and ISSOs are required to maintain a current SSP for the information systems within CFACTS. For each applicable security control, the SSP should indicate whether the control is satisfied or other than satisfied, describe how the control is implemented, and include a rationale for any tailoring decisions that have been applied to the control. A comprehensive security control implementation description should:

- Address all the requirements of the control
- Describe how each requirement and objective is met with enough detail to permit the testing of the control
- Describe the desired outcome/expected behavior of the control
- Describe where any associated process or procedures that support the controls implementation are maintained
- Identify the responsible party for ensuring that the control is properly implemented and operating as intended

It should be noted that because of the complexity of the CMS architecture many systems include multiple diverse sub-systems and/or components that may be managed and accessed by different groups depending on how the service is architected. Because of this it is important that each sub-system and/or components address the control implementation description identified in the bullet points above.
The following steps detail the CMS specific steps for documenting security control implementation descriptions using CFACTS:

- **Step 1:** Login to CFACTS and select the “Assessment & Authorization (A&A)” tab from the top menu
- **Step 2:** Expand “Authorization Package” from the downward point triangle icon
- **Step 3:** Click on “Authorization Package -Records” in the “Quick Links” list and look for the appropriate information system from the generated report by searching the available Authorization Package records generated
- **Step 4:** Once the information system has been located on the “Information System Name or Program Name” column, click on the hyperlink that corresponds to your Authorization Package system name in order to open the authorization package for the system.
- **Step 5:** Navigate to the “Controls” tab
- **Step 6:** Ensure that the controls have been allocated
- **Step 7:** Select a control by clicking on that control
- **Step 8:** Determine the Allocation Status of the control. Click “Edit” on the top of the screen
- **Step 9:** In the Control Allocation section, select the “Allocated”, “Inherited” or “N/A” radio button. Allocated controls require that all control implementation is provided by the system. Inherited controls can either be fully inherited or hybrid. Fully inherited controls inherit all the control implementation from another control provider. Hybrid controls only inherit a portion of the control and are responsible for what is not inherited
- **Step 10:** In the Inheritable and Hybrid section, determine if your system is providing the control to other systems to inherit and if it’s a hybrid control by clicking “Yes” or “No”
- **Step 11:** In the Implementation section describe how the control is implemented, who monitors or performs the control, and how often. Anything entered into the “Shared Implementation Details” field will be automatically shown as the Implementation Details in systems that inherit the control
- **Step 12:** In the “Private Allocated Controls Information” section click “Add New.” (Use this section to enter highly confidential information that should not be displayed by or available to any systems inheriting this control)
- **Step 13:** Clicking on the “Add New” in Step 12 opens the “Private Allocated Control Information: Add New Record” screen, in the screen, the user will document descriptions using the criteria listed in the three bullet points above. Click “Save” at the top
- **Step 14:** If you are providing this as an inheritable control, in the Shared Implementation Details area, document the portion of the control that is being provided to other systems. It is advisable to specifically callout whether the control is a Hybrid or not and specially state in the Shared Implementation Details what the provider is doing and what the inheriting system is required to do to fully satisfy the control
• **Step 15:** Click “Save” at the top

### 3.1.4 System Security Plan Approval

NIST SP 800-53 v4 requires that the SSP be approved by the AO or his/her designee. CMS does this through the CFACTS tool which requires the ISSO, SDM and Business Owner to approve the plan. The approval for a SSP occurs after the SSP has been reviewed and updated as part of the ATO process.

The SSP is finalized as part of the ATO process. This occurs after all the information contained within the “General”, “Security Category”, “Boundary”, “Controls”, “Assessments”, and “Authorization” tabs in CFACTS has been documented, reviewed and/or updated and the SSP plus the required supporting security artifacts have been generated. Approval of the SSP occurs after a formal security control assessment has been conducted and approved by the CMS ATO review team. Afterwards, the [CMS System Certification Authorization to Operate (ATO) Request Form](https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/CMS-System-ATO-Request-Form) has to be signed by the ISSO, SDM and Business Owner. This form is one of the three (3) key security artifacts in the ATO process, as it contains the signatures of the ISSO, SDM, and Business Owner, who act as the “Attestation Officials” and are “attesting” with their signature in the document to verify the validity, accuracy, and security posture of the FISMA system.

#### ATO Package/SSP Submittal for Approval:

The following steps detail how to validate the documentation and information in CFACTS, and prepare to submit the ATO Package which includes the SSP plus the required security artifacts for review and approval:

• **Step 1:** Refer to the CFACTS User Manual in CFACTS on how to Login and select your corresponding “Authorization Package”.

• **Step 2:** Validate the following security artifacts/documents have been uploaded to CFACTS into the appropriate CFACTS Tab:
  - System Security Plan – Authorization Tab.
  - Security Assessment Plan – Authorization Tab.
  - Security Assessment Report – Authorization tab
  - Privacy Impact Assessment (PIA) – Security Tab.
  - Interconnection Security Agreement (ISA) – Boundary Tab.
  - Information System Risk Assessment (ISRA) – Security Category Tab.
  - Contingency Plan (CP) – Security Category Tab.
  - CP Test Plan – Security Category Tab.

---

• Ensure that all POA&Ms for the system are up to date within CFACTS.

• **Step 3:** Review all security artifacts/documents to ensure the documents are complete, up to date and have been reviewed, approved, and signed.

• **Step 4:** Complete the CMS System Certification ATO Request Form and have the ISSO, SDM and Business Owner sign it.

• **Step 5:** Upload the CMS System Certification ATO Request Form to the Certification Form section of the Authorization Tab in CFACTS

• **Step 6:** In the Authorization Decision section, select “Submitted” from the pull down menu in the Authorization Package Submission Status

• **Step 7:** Remember to Click “Save” in order to commit the records to CFACTS.

**Documenting the SSP Approval:**

Once the Authorization Package has been submitted, the AO reviews the package and renders a decision. Since the SSP is a key component of the ATO package, receipt of an approved ATO also serves as a formal approval of the SSP. This decision is documented in CFACTS and an Authorization Memo is signed by the AO and must be uploaded into CFACTS by the Cyber Risk Advisor (CRA). If the ATO for the system leverages or sponsors a FedRAMP Cloud Service Provider (CSP), the CRA must forward the ATO memo to the FedRAMP PMO at info@fedramp.gov. The following steps detail how to upload the Authorization Memo into CFACTS which serves as an artifact demonstrating the SSP approval. This process assumes that the CRA has already scanned the document and has an electronic version available:

• **Step 1:** Login to CFACTS and select the “Assessment & Authorization (A&A)” tab from the top menu

• **Step 2:** Expand “Authorization Package” from the downward point triangle icon

• **Step 3:** Click on “Authorization Package -Records” in the “Quick Links” list and look for the appropriate information system from the generated report by searching the available Authorization Package records generated

• **Step 4:** Once the information system has been located click on the system name to open the authorization package for the system

• **Step 5:** Click on the “Authorization” tab

• **Step 6:** Click “Edit” at the top of the CFACTS page

• **Step 7:** Click “Add” to the right of the “Authorization Memo” in the Authorization Decision section of the Authorization tab

---

10 See the Cyber Risk Advisor FedRAMP Process document for additional details for managing Cloud Service Providers
- **Step 8:** Click “Browse” and select the authorization memo for the system. Click “Select Files” after clicking add
- **Step 9:** Click “OK”
- **Step 10:** Click “Save” at the top

### 3.1.5 System Security Plan Update and Maintenance

The CMS IS2P2 and the ARS require Business Owners to review and update the SSP at least every 365 days per FISMA and IS2P2 requirements. Please refer to the CFACTS User Manual in CFACTS for the current processes for updating the SSP within the CFACTS tool. The following steps provide the general workflow for updating the SSP in CFACTS:

- **Step 1:** Perform a comprehensive review of all the data and fields in the CFACTS Tabs for your Authorization Package:
  - General
  - Security Category
  - Boundary
  - Controls
  - Assessments
- **Step 2:** Go to the Authorization Tab in CFACTS and ensure that “Pre-assessment Progress Review” section has green check marks for all the fields for the following items:
  - Authorization Boundary
  - Security Category
  - Allocated Controls
  - Defined Implementation Details
- **Step 3:** Click on the button “Generate SSP” in the SSP section to generate your SSP. A new SSP will be generated for the date and time you execute this action. This is a “time stamp” of the data you are pulling from CFACTS that is contained within this SSP document
- **Step 4:** When the Authorization Package: Export Options window opens, generate your SSP using the SSP Report Template in Microsoft® Word
- **Step 5:** Save your SSP Microsoft® Word document to the specified directory location on your computer/network. Please remember where you saved this file
- **Step 6:** Review the generated SSP for completeness and accuracy
- **Step 7:** Upload the SSP to the SSP Attachments area of the SSP section. Use the following naming convention {System Name} _SSP_ (date generated} e.g., OCISO Inheritable Controls_SSP_04252016
3.1.6 **Plan/Coordinate with Other Organizational Entities (PL-2(3))**

CMS must plan and coordinate security-related activities impacting the information system with the affected internal or external stakeholders, meet up with groups, or organizations before conducting such activities in order to reduce the impact on other CMS organizational entities. These stakeholders, groups, or organizations could include those involved with security-related activities, or providing services or support (such as Trusted Internet Connection (TIC), or those involved in the Continuity of Operations Plan (COOP)).

The table below outlines the CMS organizationally defined parameters (ODPs) for PL-2(3).

<table>
<thead>
<tr>
<th>Control</th>
<th>Control Requirement</th>
<th>CMS Parameter</th>
</tr>
</thead>
</table>
| PL-2(3) | The organization plans and coordinates security-related activities affecting the information system with [Assignment: organization-defined individuals or groups] before conducting such activities in order to reduce the impact on other organizational entities. | The organization plans and coordinates security-related activities affecting the information system with affected internal or external stakeholders, groups, or organizations before conducting such activities to reduce the impact on other organizational entities. Stakeholders associated with the following security-related activities:  
- Security Control Assessors (SCAs)  
- Auditors (e.g., Chief Financial Officer (CFO) Audits, and Annual FISMA audits)  
- Organizations providing or associated with Continuous Diagnostics and Mitigation (CDM) [i.e., the CMS CCIC (SOC)]  
- Security Awareness Training (SAT) Instructors  
- Hardware and Software Maintenance Administrators  
- Patch Management/Configuration Management Administrators/Coordinators  
- Contingency Plan/Information Technology Continuity Plan (CP/ITCP) Testing facilitators/participants  
- Incident Response Testing facilitators/participants |

The following steps detail a process for coordinating security related activities with internal and external stakeholders.
• **Step 1:** Identify all the relevant stakeholders for the security related activity
• **Step 2:** Establish a primary method of communication. Possible methods of communication include emails, face to face meetings, and teleconferences
• **Step 3:** Communicate with all relevant stakeholders using the primary method of communication identified in Step 2 above. Introduce the security related activity and describe the areas for which you are requesting input/support from each stakeholder. Be sure to generate an artifact documenting this interaction (e.g., email trails, meeting minutes, etc.)
• **Step 4:** Issue follow up communications as necessary. You may use other methods of communication aside from the primary method identified in Step 2 but you must generate an artifact documenting the interaction (e.g., email trails, meeting minutes, etc.)

### 3.2 Rules of Behavior (PL-4)

Rules of Behavior (RoB) clearly delineates responsibilities and the expected behavior of all individuals with access to the system.

The table below outlines the CMS organizationally defined parameters (ODPs) for PL-4.

<table>
<thead>
<tr>
<th>Control</th>
<th>Control Requirement</th>
<th>CMS Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>PL-4</td>
<td>The organization:</td>
<td>The organization:</td>
</tr>
<tr>
<td></td>
<td>c. Reviews and</td>
<td>c. Reviews and</td>
</tr>
<tr>
<td></td>
<td>updates the rules</td>
<td>updates the</td>
</tr>
<tr>
<td></td>
<td>of behavior</td>
<td>rules of</td>
</tr>
<tr>
<td></td>
<td>[Assignment:</td>
<td>behavior at</td>
</tr>
<tr>
<td></td>
<td>organization-defined frequency];</td>
<td>least every</td>
</tr>
<tr>
<td></td>
<td></td>
<td>three years</td>
</tr>
</tbody>
</table>


The following steps detail the CMS process for ensuring that CMS users review and acknowledge the Rules of Behavior.

• **Step 1:** The rules of behavior have been incorporated into the annual Security and Privacy Awareness Training, and all EUA users must take the Computer Based Training (CBT) located at [https://www.cms.gov/cbt/forms/isspa.aspx](https://www.cms.gov/cbt/forms/isspa.aspx). The training is taken by all EUA users initially prior to account issuance and annually thereafter to maintain an active CMS account

• **Step 2:** Each year based on the date of account issuance each user receives an email requiring them to review and complete the annual CBT

• **Step 3:** Training records are maintained using the CBT database and include the Unique Identification (UID) and the date the individual last completed the training

---

• **Step 4:** Use of Social Media/Networking Sites and Posting Organizational Information on Public Websites have been incorporated in the annual Security and Privacy Awareness Training and the RoB is electronically signed as the last step of that training. Failing to complete the CBT training will result in the user having his/her credentials revoked.

Additional information on rules of behavior training have been incorporated into Chapter 2 of the Risk Management Handbook on Awareness and Training (AT)\(^\text{12}\).

### 3.2.1 Social Media and Networking Restrictions (PL-4(1))

CMS includes in the RoB explicit restrictions on the use of social media/networking sites and posting organizational information on public websites. The rules of behavior have been incorporated into the annual Security and Privacy Awareness Training which is delivered via CBT. Refer to section 3.2 of this document for procedures for completing the CBT.

### 3.3 Information Security Architecture (PL-8)

This control addresses actions taken by CMS organizations in the design and development of information systems. The CMS information security architecture at the individual information system level is consistent with and complements the more global, organization-wide information security architecture. The CMS information security architecture includes:

- Architectural Description
- Placement/Allocation of Security Functionality
- Allocation of Security Controls
- Security-related information for external interfaces, information being exchanged across the interfaces
- Protection mechanisms associated with each interface.

In addition, the security architecture can include other important security-related information, for example, user roles and access privileges assigned to each role, unique security requirements, the types of information processed, stored, and transmitted by the information system, restoration priorities of information and information system services, and any other specific protection needs. The table below outlines the CMS organizationally defined parameters (ODPs) for PL-8.

<table>
<thead>
<tr>
<th>Control</th>
<th>Control Requirement</th>
<th>CMS Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>PL-8</td>
<td>The organization: b. Reviews and updates the information security architecture [Assignment: organization-defined frequency] to reflect updates in the enterprise architecture;</td>
<td>The organization: b. Reviews and updates (as necessary) the information security architecture no less often than every three (3)</td>
</tr>
</tbody>
</table>

---

Control | Control Requirement | CMS Parameter
--- | --- | ---
 |  | years and whenever changes are made to the enterprise architecture; | 

The CMS TRA articulates the technical architecture of the CMS processing environments. As a foundation document, the CMS TRA is designed to assist all agency business partners in developing to, transitioning to, and maintaining the CMS Processing Environments in accordance with CMS’s enterprise technical architecture. The CMS enterprise technical architecture supports five critical technical objectives that enable the agency’s healthcare mission:

- Secure the CMS operating environment
- Allow for the efficient allocation of CMS workloads across data centers
- Provide appropriate and sufficient disaster recovery and business continuity capability
- Facilitate the migration and transition of CMS business owner applications into new Processing environments
- Build an enterprise technical architecture that anticipates and responds to CMS’s mission and business needs