
**Centers for Medicare & Medicaid Services**
**Information Security and Privacy Group**

# CMS Information Systems Security Officer (ISSO) Appointment Letter (Template)

**Version 2.0**

**January 21, 2020**

# Record of Changes

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

| Version Number | Date | Author/Owner Name | Description of Change |
|---|---|---|---|
| **1.0** | August 11, 2016 | ISPG | Final |
| **2.0** | January 21, 2020 | ISPG | Added cover letter providing guidance for the ISSO role. Included Appendix listing knowledge, skills, and abilities from NICE Framework. Added questions associated with the ISSO Initiative for training and engagement. Comments from ISSOs, ISPG incorporated. |

# Selecting the ISSO

According to the National Institute of Standards and Technology's Guide for Applying the Risk Management Framework to Federal Information Systems, NIST Special Publication 800-37, the Information System Security Officer (ISSO) is an "individual with assigned responsibility for maintaining the appropriate operational security posture for an information system or program".

## Guidance

*The ISSO role at CMS is responsible for both the technical and the business evaluations for securing information and systems. The role requires the skills necessary to evaluate technical solutions from an information security perspective and to determine the business risks in order to justify decisions to both the Business Owner and the technical support staff.*

The CMS Information Systems Security and Privacy Policy (IS2P2) and the HHS Information Systems Security and Privacy Policy (IS2P) contain the duties and responsibilities of the ISSO role (IS2P section 19, IS2P2 section 3.4.7). Under the IS2P2 section, 3.3.1 the Chief Information Officer (CIO) is responsible for defining the minimum ISSO qualifications commensurate with CMS information sensitivity. Under section, 3.3.2 the Chief Information Security Officer (CISO) is responsible for approving the appointment of the ISSO.

The CMS Program Executive, also known as the Business Owner, is responsible under section 3.4.1 of the IS2P2, to nominate appropriately qualified ISSO appointees, as defined under FISMA, to the CISO for approval. NIST Special Publication 800-37 Rev 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Appendix D characterizes the system security officer is "generally responsible for aspects of the system that protect information and information systems from unauthorized system activity or behavior to provide confidentiality, integrity, and availability.

See the Appendix of this Template for helpful information for ISSO selection.

## Instructions for ISSO Appointment Letter Completion and Submission

The ISSO appointee completes questions in Section 1 & 2, and the top box in Section 3, signs the form and then submits it to their Program Executive/Business Owner.

The Program Executive/Business Owner completes all appropriate areas in Section 3, signs, and dates the form and returns it to the appointee.

The ISSO appointee submits the form to the Cyber Risk Advisor (CRA) for the assigned FISMA system(s) for review and acceptance by the CISO.

After the Appointment letter is accepted by the CISO, it is uploaded to the CMS Risk Governance tool, CFACTS, to the applicable FISMA system.

# Experiences and Qualifications

The answers to the following questions will provide information on the ISSO appointee's experience and qualifications (answer in one or two sentences, use separate page if needed), to assist ISPG with identifying effective training opportunities.

1. Briefly describe your experience in computer/information security.

2. Do you possess experience assessing or implementing security and privacy controls? If yes, please briefly describe.

3. Please list any security related certifications you currently hold (CISSP, GIAC, Security +, etc.).

4. Please list any security and/or privacy related training courses you have taken and any you would recommend.

5. Please indicate your level of experience in the following security topics from 1 (None) to 5 (Expert). (*see Appendix for related NICE Knowledge, Skills, Abilities (KSAs*):

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| NIST Security Related Guidance | ◉ | ○ | ○ | ○ | ○ |
| Acceptable Risk Safeguards (ARS) | ○ | ○ | ○ | ◉ | ○ |
| System Security Plans | ○ | ○ | ○ | ○ | ◉ |
| CMS Incident Response Procedures | ○ | ○ | ○ | ◉ | ○ |
| Plans of Action and Milestones | ○ | ○ | ○ | ◉ | ○ |
| Contingency Planning | ○ | ○ | ◉ | ○ | ○ |
| Risk Assessments | ○ | ○ | ○ | ◉ | ○ |
| Security Impact Analysis | ○ | ○ | ◉ | ○ | ○ |

| | | | | | |
|---|---|---|---|---|---|
| Privacy Impact Assessment | ○ | ○ | ○ | ○ | ◉ |
| FedRamp/Cloud Service Providers | ○ | ○ | ◉ | ○ | ○ |
| Incident Response | ○ | ○ | ◉ | ○ | ○ |

ISSO Acknowledgment of Responsibilities

I, (**Full name**), have been formally appointed as a CMS Information Systems Security Officer (ISSO). I understand it is the responsibility of the ISSO to maintain the appropriate operational security posture of the information system by fulfilling all of the responsibilities identified in the CMS Information Systems Security and Privacy Policy (CMS IS2P2) Section 3.4.7, *Information Systems Security Officer*; and HHS Information System Security and Privacy Policy Appendix A Section 19, *ISSO* including but not limited to the following:

- Complete the security categorization for the information system using the CFACTS tool
- Complete and maintain the System Security Plan using the CFACTS tool
- Ensure a Security Assessment in accordance with CMS policy has been scheduled and completed in a timely manner
- Develop, document and maintain an inventory of hardware and software components within the authorization boundary
- Coordinate the development of a Contingency Plan and ensure the plan is tested and maintained in accordance with CMS policy
- Coordinate with the Information System Owner (ISO), Business Owner, and Cyber Risk Advisor (CRA) to manage information security and privacy risk
- Monitor and update all Plan of Action and Milestones (POA&Ms) in accordance with the CMS Risk Management Handbook (RMH)
- Submit recommendations to the CRA for system configuration deviations from the required baseline
- Identify the information security and privacy controls provided by the applicable infrastructure that are common controls for information systems
- Coordinate with the, ISO, Business Owner, and CRA to meet all collection, creation, use, dissemination, retention, and maintenance requirements for PII, PHI, and FTI in accordance with the Privacy Act, E-Government Act, and all other applicable guidance
- Coordinate with the Business Owner, Contracting Officer, ISO, and CISO to ensure that all requirements specified by the ARS and the RMH are implemented and enforced for applicable information and information systems
- Report and manage IT Security and Privacy Incidents in accordance with the RMH and other applicable federal guidance

ISSO Signature: Date: [1]

[1] This document may be updated as necessary to reflect changes in policy or process and may require resubmission. If you have any questions regarding further processing or the content of this document, please contact the ISPG at ISPG_Policy_Mailbox@cms.hhs.gov or CISO@cms.hhs.gov.

# CMS Information Systems Security Officer (ISSO) Appointment

| | |
|---|---|
| **ISSO Name:** | |
| **Title:** | |
| **CMS Component:** | |
| **Group/Division:** | |
| **Telephone Number:** | |
| **Email Address:** | |
| **Assigned FISMA System(s):** | |
| **Effective Date(s):** | |

**Affiliation (select one)**

CMS Employee

CMS Contractor (if selected, complete next two lines)

Name of Contract:

Start/End Date: Contract #:

**Program Executive**[2]

Name:

Title:

Signature: Date:

**Review and Approval (CMS Chief Information Security Officer or Designated Approver)**

Name Title:

Signature: Date:

Expiration Date: [3]

[2] See Section 3.4.1 of the CMS Information Systems Security and Privacy Policy located on the Information Security and Privacy Library: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html

[3] Appointment expires after two years from date signed or when changes in policy or process require resubmission.

# Appendix

This appendix provides information to consider when selecting an individual for the role of ISSO. Some redundancy may occur as the information selected is from multiple sources and is retained to stress importance.

## Qualifications

The ISSO role will often times require a solid technical background, good management skills, and the ability to deal well with people at all levels from top management to individual users. Perspective in-house ISSOs should have an introductory level of knowledge of their component's business process and finances, experience with network and systems administration, a familiarization with network networking protocols and operating systems and an intermediate level of knowledge of security concepts. It is recommended that ISSOs:

- Learn the security planning and administrative security procedures for systems that process sensitive information such as Protected Health Information (PHI) and Personally Identifiable Information (PII);
- Understand the implementation and enforcement of CMS' Information System Security and Privacy Policies and Practices;
- Know the concerns and requirements that determine the administration and management of physical, system, and data access controls based on the sensitivity of the data processed and the corresponding authorization requirements;
- Learn the identification, analysis, assessment, and evaluation of information system threats and vulnerabilities and their impact on their component's critical information infrastructures;
- Identify management, technical, personnel, operational and physical security controls;
- Understand basic system development life cycle paradigms and applies to information system security; and
- Are familiar with the Role Based Training requirements found in Policy, i.e.; IS2P2 & IS2P.

## Knowledge, Skills, Abilities (KSAs)

The following KSAs can be attributable to the CMS ISSO role. They were distilled from the KSAs associated with the Information Systems Security Manager (ISSM) work role from the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework). The NICE Framework provides a blueprint to categorize, organize, and describe cybersecurity work into Categories, Specialty Areas, Work Roles, tasks, and knowledge, skills, and abilities (KSAs). The NICE Framework provides a common language to speak about cybersecurity roles.

## Knowledge:

- ✓ Knowledge of risk management processes (e.g., methods for assessing and mitigating risk)
- ✓ Knowledge of computer networking concepts and protocols, and network security methodologies
- ✓ Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data
- ✓ Knowledge of enterprise incident response program, roles, and responsibilities

## Skills:

- ✓ Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes
- ✓ Skill in developing and applying security system access controls
- ✓ Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.)
- ✓ Skill in recognizing vulnerabilities in security systems. (e.g., vulnerability and compliance scanning)
- ✓ Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes

## Ability:

- ✓ Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation)
- ✓ Ability to review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network

# Experience

- Work experience in computer security or
    - Attendance and completion of a computer security training course with certification or
    - Work experience in a computer related field
- Familiarization with the information systems of the component / office
- A degree in computer science, mathematics, electrical engineering, or a related field

- Familiarization with networking protocols and operating systems and an intermediate level of knowledge of security concepts with emphasis on data protection and integrity is preferred
- An understanding of or experience with incident response processes and their importance
- Developing and applying system access control

## Business Knowledge

A goal of the ISSO is to help the Business Owner securely provide the services intended by the IT system. Successfully accomplishing this goal, the ISSO should know and understand their component's business processes and how the system supports that business. This knowledge is critically applied during the construction and testing of the system's Contingency Plan.

## Core Competencies

The ISSO role supports the confidentiality, integrity, availability, reliability, and non-repudiation of CMS' information contained in and transmitted from systems and networks by implementing security laws, regulations, policies, standards, and control techniques.

### Some Key Behaviors:

- Uses knowledge of continuity assurance principles, methods, and practices to plan, implement and ensure continuous service;
- Assesses risks associated with systems and information including identifying, understanding, and resolving associated vulnerabilities;
- Considers privacy, security and accessibility of government websites;
- Keeps up to date on standards and determines or recommends levels of security protection required to protect and close exposure/risk to systems and information, in accordance with organization and federal standards;
- Uses the concepts of confidentiality, integrity and availability as applied to information systems security;
- Recommends cost effective methods to reduce risks to systems and information;
- Reviews the types of and uses or recommends the most effective security controls as directed by Federal policies and procedures;
- Ensures procedures for detecting, reporting and responding to security incidents are consistent with and follow standards and guidelines issued by applicable governing entities and regulations;
- Identifies and evaluates resources needed to achieve acceptable levels of security and to remedy deficiencies based on system criticality and information sensitivity; and
- Clearly understand the implications of legislation, regulations, and standards related to information assurance and security.