CMS Information Security and Privacy Overview

"Holding Ourselves to a Higher Standard"

Overview

The CMS information security and privacy virtual handbook is intended to serve as your "one stop" resource for all things related to CMS information security and privacy policy. On this page, you'll find links to all CMS information security and privacy policies, standards, procedures, and guidelines as well as computer based training, user ID assignment and complete instructions on what to do if you suspect that a security incident has occurred. The links on the left hand side of the page provide supplementary guidance on CMS policy, however, for a brief snapshot and high-level overview of some of our core programs, please take a look at the information provided below:

Security Incidents

Known or suspected security or privacy incidents involving CMS information or information systems must be reported immediately to the CMS IT Service Desk by calling 410-786-2580 or 1-800-562-1963, or via e-mail to CMS_IT_Service_Desk@cms.hhs.gov. Additionally, please contact your ISSO as soon as possible and apprise them of the situation.

CMS Information Security and Privacy Contract Requirements

CMS has modified its contracts and solicitations for the incorporation of a CMS Information Security clause/provision to safeguard information and information systems that support the operations and assets of the agency, including those provided or managed by contractors (including subcontractors) on behalf of the agency. Click here: /Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library

Security in the Systems Development Lifecycle (SDLC)

Early consideration of security and its subsequent integration into every aspect of the system development life cycle not only ensures the long-term protection of sensitive information, it also prevents costly, duplicative effort after the project's completion. If you are a developer and you have any questions regarding how to integrate security into your product, the "System Lifecycle Framework" provides complete details related to the CMS Target Life Cycle (TLC). The CMS Information Technology - General document, may also provide useful supplemental guidance.

Security Assessment and Authorization (SA&A)

The Security Assessment and Authorization (SA&A) process, formerly known as Certification and Accreditation (C&A), is the methodology by which an organization establishes and then demonstrates a sound information security posture for a specific system. Throughout this rigorous process, the Information System Security Officer (ISSO) will serve as your primary point of contact for system security and privacy issues and policy guidance.   ISSOs act as an important liaison between the CMS Chief Information Security Officer (CISO) and the many business components within CMS.

Security Control Assessment (SCA)

The Security Control Assessment, formerly known as a Security Test and Evaluation (ST&E), is a detailed evaluation of the controls protecting an information system. The security control assessment determines the extent to which controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Requirements for control assessments are described in the CMS Acceptable Risk Safeguards (ARS) in the Security Assessment and Authorization (CA) section of the document.

Information Security and Privacy Library

Almost any question you have related to the CMS Information Security program may be answered in one brief visit to the CMS Information Security and Privacy Library. Use the convenient search tool to quickly locate relevant policies, procedures, templates and guidelines.

The National Institute of Standards and Technology (NIST) established many of the foundational security standards that help protect our Nation's Information Technology infrastructure. A Complete listing of NIST publications can be found at www.csrc.nist.gov. (See Related Links below)

Spotlight

The CMS "Spotlight" portal keeps you up-to-date with the latest changes to CMS and related Federal policies and also highlights many of the foundational components of the CMS information security and privacy program. Here you will find many of the most current, common standards, procedures, and policy documents applicable to CMS.

Enterprise User Administration (EUA)

A CMS User ID serves as your "virtual security badge," for CMS Networks, granting you access to information and resources that you are authorized to see and preventing access to information and resources that you are not authorized to see. Management of most CMS User ID's is accomplished through the Enterprise User Administration (EUA) system. Additional information regarding the system can be found under the "CMS System User Information" heading. If you would like information on the Medicare Advantage and Prescription Drug Plans (MAPD) as well as the CMS enterprise Identity Management and Authentication system (IACS), click here IACS.

Computer Based Training (CBT)

Initial computer based training helps to establish a foundation of information security understanding and competency across the extended CMS enterprise and subsequent refresher training ensures that the foundation remains sound over time. Computer based training (CBT) is mandatory for most users of CMS Information Systems and is normally conducted upon initial CMS User ID assignment and then annually when recertification of the CMS User ID is required. For additional details about the CBT program, please select the "Computer Based Training" tab on the left hand side of the page. Access to the "Information Security CBT" is at the bottom of the page and is restricted to authorized users only.

CMS FISMA Controls Tracking System (CFACTS)

CFACTS is the CMS Governance, Risk and Compliance tool used as a repository to manage the security and privacy requirements of its information systems. This platform provides a common foundation to manage policies, controls, risks, assessments and deficiencies across the CMS Enterprise. Users may access the CFACTS by selecting the following link CFACTS.

CISO Mailbox

Do you have a question or concern related to CMS information security or privacy? Send an email to the CISO Team at CISO@cms.hhs.gov regarding information security, or an email to Privacy@cms.hhs.gov for questions regarding privacy.

Information Systems Security and Privacy Policy (IS2P2)

The Information Security and Privacy Group (ISPG) updated the Information Systems Security and Privacy Policy (IS2P2) in 2019. These updates are documented in the document titled, "IS2P2 2.0 Updates", and can be found on the Information Security and Privacy Library. The IS2P2, as amended, is located on the CIO Library.

This Policy defines the framework under which CMS protects and controls access to CMS information and information systems. This Policy provides direction to all CMS employees, contractors, and any individual who receives authorization to access CMS information technology (IT) systems; systems maintained on behalf of CMS; and other collections of information to assure the confidentiality, integrity, and availability of CMS information and systems.