

Final

Centers for Medicare & Medicaid Services



Centers for Medicare & Medicaid Services
Information Security and Privacy Group

CMS Privacy Impact Assessment (PIA) Standard Operating Procedures

Final

Version 1.0

August 8, 2019

Table of Contents

Record of Changes	ii
Effective Date/Approval	iii
Table of Contents	iv
1. Introduction	1
2. What is a Privacy Impact Assessment	1
2.1 Defining the Different Types of PIAs	1
2.2 Personally Identifiable information (PII)	2
2.3 The Privacy Act and the PIA.....	2
3. When to Conduct a PIA	3
3.1 Revision Cycle	4
3.2 What is considered a major change.....	4
4. Overview of Roles and Responsibilities	5
4.1 HHS Chief Information Officer (CIO)\Senior Agency Official for Privacy (SAOP).....	5
4.2 CMS Senior Official for Privacy (SOP).....	5
4.3 CMS System Owner/Business Owner.....	6
4.4 CMS Privacy Advisor	6
4.5 CMS Cyber Risk Advisor (CRA).....	6
4.6 CMS Information System Security Officer (ISSO)	7
5. Privacy Impact Assessment Workflow	7
6. Question-by-Question guidance and resources	8
7. Third-Party Websites and Applications (TPWA)	9
Appendix A. Tips for Writing an Effective PIA	11
Appendix B. Additional Guidance & Resources	12
Appendix C. References	13

1. Introduction

The E-Government Act of 2002, the Office of Management and Budget (OMB) and Health and Human Services (HHS) policy all require CMS to complete PIAs on all systems and electronic information collections maintained by or on behalf of the agency.¹ Per Circular OMB A-130, the PIA development, review and revision process allows senior officials to manage the privacy risks associated with in an information system and to make recommendations regarding the authorization of the system.

As established by HHS and the CMS Information Systems Security and Privacy Policy (IS2P2), the CMS Senior Official for Privacy (SOP) must establish a policy framework to facilitate the development and maintenance of PIAs in accordance with federal and HHS requirements.

2. What is a Privacy Impact Assessment

The PIA is a critical tool for spotting privacy risks and compliance with federal regulations or laws, tracking implementation of privacy controls, identifying instances where the Agency collects or handles Personally Identifiable Information (PII) and/or Protected Health Information (PHI) and for identifying CMS systems subject to the Privacy Act of 1974. HHS has developed two different analytical questionnaire documents for use in conducting PIAs, the PIA and the Third Party Website Assessment (TPWA).

2.1 Defining the Different Types of PIAs

As defined by HHS below are the definitions for the different types of PIAs and the requirements:

Privacy Impact Assessment (PIA): an analysis of how information is handled to:

1. Ensure handling confirms to applicable legal, regulatory, and policy requirements regarding privacy;
2. Determine the risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, and disclosing, and disposing of PII in an electronic information system; and
3. Examine and evaluate protections and alternate processes for handling information to mitigate potential privacy concerns.

A PIA is both an analysis and a formal document detailing the process and the outcome of the analysis. PIAs must be reviewed at least every three years and/or upon a major change to the IT system or electronic information collection. Major changes are discussed in more details in section 5.2.

¹ Although neither Section 208 of the E-Government Act, nor OMB's implementing guidance mandate agencies conduct PIAs on electronic systems containing PII solely related to Federal employees (including contract employees), OMB encourages agencies to scrutinize their internal business processes and the handling of personally identifiable information about employees to the same extent they scrutinize processes and information handling procedures involving information collected from or about members of the public (OMB Memorandum 03-22, Section ILB.3.a.).

If the PIA collects PII only about CMS employees and direct contractors then the form is an internal PIA. PIAs that are internal are not published on the HHS website and are not subject to the three-year review requirement. However, PIAs must be updated when a major change is planned for an IT system or electronic information collection.

Privacy Threshold Analysis (PTA): an analysis performed in lieu of the formal PIA where the information handled in the IT systems and electronic information collections do not collect, disseminate, maintain, or dispose of PII. Since HHS uses an interactive form for PIAs, a separate document is not necessary to complete a PTA. PTAs are not published on the HHS website and are not subject to the three year review requirement. PTAs must be updated upon a major change to the IT system or electronic information collection. It is possible that a major change could result in a PTA meeting the threshold to be a PIA (e.g., the addition of PII).

Third Party Website Application (TPWA) PIA: an analysis of agency use of third-party websites or application technologies such as social media used by CMS to communicate and engage with members of the public. The TPWA PIA has different questions that are based on the specific risks and compliance requirements for TPWAs as outlined by OMB M-10-23. However, both the PIA and TPWA PIA require approval from HHS and are published on the HHS public webpage.

2.2 Personally Identifiable information (PII)

The federal government has adopted a broad definition of what is “personally identifiable information.”² PII is information that can be used to identify an individual directly or indirectly when information is linked together. When combined with other information, the integrity of records relating to a person can be compromised by permitting unauthorized access to or unauthorized disclosure of records. Examples of what is considered PII include but is not limited to Social Security Number (SSN), name, address, passport number, biometric identifiers, or medical records.

Information about an individual is PII whether the information is publicly available, provided voluntarily or collected by mandate. For example, some information about a patient can be found publicly available through other mediums but this does not negate that the information is still considered PII when collected, stored, maintained or shared with CMS.

2.3 The Privacy Act and the PIA

During the process of conducting a PIA, it is possible to discover that information is being collected, used, and stored by their system and retrieved by a personal identifier to make determinations about members of the public and/or provide services to them. If this is the case, then the information system may be a system of records (SOR) and subject to the Privacy Act of 1974.

² Taken from m-17-12, PII refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad.

A system is considered a Privacy Act System of Records, if it: (1) receives and retains personal identifiers (PII), and, (2) the agency “does, in fact, retrieve records about individuals by reference to some personal identifier,” for example, querying the system by use of an individual’s name. There is a distinction between capabilities versus actual use; the fact that a system provides the ability to search by any term does not constitute actual retrieval by PII. Therefore, the Privacy Act requirement is triggered by the collection of information that is actually retrieved by a personal identifier.

The Privacy Act also requires agencies to publish Systems of Records Notices (SORNs) in the Federal Register that describe the categories of records on individuals that they collect, use, maintain, and disseminate information on. Often times the applicable SORN for a system will have content that can answer some of the questionnaire responses in the PIA such as categories of records and authorities for maintaining information.

However, it is important to note that completing a PIA does not fulfill the Privacy Act requirement to complete a SORN:

- A PIA is used to analyze the impact of the technology that is using personally identifiable information.
- A SORN is used to provide notice to members of the public that their information is being used by the agency.

Discussion on the process for developing, modification and publishing a SORN is beyond the scope of this document. See the CMS Privacy Handbook for guidance on SORNs.

3. When to Conduct a PIA

Information system PIAs are also part of the Security Assessment and Authorization (SA&A) process for systems at CMS; thus, the PIA, must be reviewed and revised as necessary, as part of an information system initial authorization and reauthorization process. As stated from OMB M-03-22, “OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002”, the following are situations which require a PIA:

- A new information system or electronic information collection is planned to be in operation requires conducting a PIA.
- Information Collection Requests (ICRs) that collects information from 10 or more members of the public typically fall under the Paperwork Reduction ACT (PRA). A new PIA may be required for an information collection that is not covered by an existing PIA.
- A major change to how information is collected, stored, maintained or shared occurs for an information system or electronic information collection as described in section 5.3 below.
- A PIA is close to expiring, which will require an update to the form. If the information system is going through an ATO, the PIA needs to be active and not expired/incomplete before going into operation.³

³ From Section 208(b) of the E-Government Act, there is a requirement that agencies, absent an applicable exception under that section, to conduct a PIA before developing or procuring an information system that collects, maintains, or disseminates information. Currently HHS policy states that before an Authorization to Operate (ATO) is to be granted, the PIA needs to be signed by HHS.

As stated previously, HHS also requires PIAs to be conducted every three years if the information system collects, maintains, stores or shares information on individuals that are not federal employees or direct contractors of CMS.

3.1 Revision Cycle

The PIA development, review, and revision process allows the CMS SOP to confirm that appropriate privacy controls are in place to manage the privacy risks associated with an IT system and to make recommendations regarding the authorization of that IT system. System/Business Owners and Information System Security Officers (ISSO) must review, revise as necessary, and submit PIAs for re-approval three years from the last HHS approval date.

PTAs, PIAs, and Internal PIAs must also be reviewed, updated, and re-approved whenever a major change to an IT system, a change in CMS privacy practices, or another factor alters the privacy risks associated with the use of a particular IT system or electronic information collection.

PTAs and Internal PIAs are not reviewed on the three-year cycle and are not on a three-year expiration date like standard PIAs. However, PTAs and Internal PIAs are required to be updated and re-approved when a major change occurs and should be reviewed during the SA&A process, though if no major changes occurred the PTAs and Internal PIAs do not require new signatures.

3.2 What is considered a major change

A major change is something that alters the privacy risk associated with the use of a particular IT system. An example of a major change that would require an update to the PIA is a decision to collect social security numbers for an information system that previously was not collecting social security numbers. According to OMB M-03-22, PIAs should be reviewed following the major changes including, but not limited to:

- **Conversions:** A conversion from paper-based methods to electronic systems (e.g. records currently in paper form will be scanned or otherwise added into a system);
- **Anonymous to Non-Anonymous:** When the system's function, as applied to an existing information collection, changes anonymous information into PII.
- **Significant System Management Changes:** In the case that new uses of an existing IT system, including application of new technologies, significantly change the process of managing PII in the system.
- **Significant Merging:** When agencies adopt or alter business processes so that government databases holding PII are merged, centralized, matched with other databases, or otherwise significantly manipulated
- **New Public Access:** When user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system, which can be accessed by the public
- **Commercial Sources:** When PII is obtained from commercial or public sources and is systematically integrated into the existing information systems databases

- **New Interagency Uses:** When agencies work together on shared functions involving significant new uses or exchanges of PII
- **Internal Flow or Collection:** When alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional PII; and
- **Alteration in Character of Data:** When new PII added to a collection raises the risk to personal privacy, such as the addition of health or privacy information.

4. Overview of Roles and Responsibilities

The following roles identified in this section are responsible in different areas for the development and completion of PIAs at CMS.

4.1 HHS Chief Information Officer (CIO)\Senior Agency Official for Privacy (SAOP)

At HHS, the CIO is designated as the SAOP and provides the overall program structure for the completion of PIAs across all operating divisions. Responsibilities include, but are not limited to the following:

- a. Develop a standard form for HHS PIAs.
- b. Review PIAs from all operating divisions (OPDIV) for adequacy, consistency and compliance with federal and HHS requirements.
- c. If the PIA meets HHS's requirements, the PIA is signed by the SAOP, which finalizes the PIA for a period depending on the type of PIA.
- d. Ensure all PIAs are published and made publicly available on HHS.gov.

4.2 CMS Senior Official for Privacy (SOP)

At CMS, the SOP is the lead privacy official responsible for administering the agency PIA process and providing direction for the CMS privacy program. Responsibilities include, but are not limited to the following:

- a. Establish a CMS specific framework for the development and completion of PIAs in accordance with federal and HHS requirements.
- b. In coordination with the Final Approver⁴ whom assists the SOP, review and approve all PIAs for completion and consistency prior to submission to the HHS SAOP.
- c. Unresolved privacy risks and other potential issues should be addressed before submission to the CMS SOP for final review.⁵
- d. The SOP signs the PIA on behalf of CMS once the PIA satisfies federal and HHS requirements but will require HHS's signature before finalization and publication to the HHS website.

⁴ The Final Approver for the purpose of the CMS privacy program works on behalf of the SOP to review PIAs for compliance and inconsistencies. The Final Reviewer also communicates with HHS on the status, review, signature and publication of PIAs.

⁵ The SOP/Final Approver is not responsible for performing an in-depth review of the PIA. The PIA should not have glaring issues such as unanswered questions, outstanding privacy risks, poor grammar or misspellings prior to submission. The ISSO, CRA and Privacy Advisor will need to coordinate to ensure the PIA is completed and all privacy risks are addressed before submission to the SOP/Final Approver and HHS.

4.3 CMS System Owner/Business Owner

The Information System Owner or Business Owner includes individuals who are responsible for the IT systems or electronic information collections. Some of the outlined responsibilities below are delegated to the Information Systems Security Officer (ISSO) on behalf of the System/Business owner. Responsibilities include, but are not limited to the following:

- a. Review, revise as necessary, and submit PIAs for re-approval whenever a change to an IT system, a change in CMS practice, or another factor alters the privacy risks associated with the use of the IT system or electronic information collection.
- b. Allocating proper resources to permit identification and remediation of privacy risks and weaknesses identified on PIAs.
- c. Review, revise as necessary, and submit PIAs for re-approval three years from the last approval date, and as part of the authorization process as required.
- d. Complying with all relevant Privacy Act requirements regarding any system of records, including, but not limited to, providing individuals with procedures for access and amendment of records.
- e. Ensure all artifacts are in place as needed such as a Computer Matching Agreement (CMA), Information Exchange Agreements (IEA), or any other agreement when sharing information.
- f. The System/Business Owner can sometimes conduct and develop the PIA in the place of an ISSO.

4.4 CMS Privacy Advisor

The Privacy Advisor has in-depth knowledge of identifying privacy risks and requirements in the PIA. Responsibilities include, but are not limited to the following:

- a. Review component PIAs for accuracy, consistency and compliance; coordinating with the Cyber Risk Advisor to identify any outstanding privacy risks prior to submission to the CMS SOP.
- b. Ensuring answers provided in the PIA are consistent with the HHS PTA and PIA Writers Handbook. In addition, checking for Privacy Act implications and checking for grammatical mistakes or incomplete responses.
- c. Provide input and guidance as needed regarding any other privacy weaknesses as identified.

4.5 CMS Cyber Risk Advisor (CRA)

The CRA is responsible for coordinating the drafting and review process of the PIA with the CMS office or center in which they are representing. Responsibilities include, but are not limited to the following:

- a. Communicate with System/Business Owners' through the authorization process including ensuring the PIA is a part of the security package.
- b. Review PIAs submitted by the ISSO or System Owner for potential security and privacy risk, this can include for example:

- Checking that information in the PIA matches other artifacts in the ATO package as needed, including checking for grammatical mistakes or incomplete responses.
 - Ensuring the answers provided in the PIA are consistent with the HHS PTA and PIA Writers Handbook.
- c. Coordinating with the Privacy Advisor for the review of the PIA and identifying any potential privacy risks.
 - d. Review PIAs sent back from the SOP and/or HHS and coordinate with the ISSO and Privacy Advisor to resolve the outstanding comments as needed.
 - e. Once the PIA is satisfactory in coordination with the Privacy Advisor, submit the PIA for approval to the CMS SOP.

4.6 CMS Information System Security Officer (ISSO)

The ISSO has the responsibility of providing oversight, developing documentation and ensuring the completion of the Security Assessment and Authorization (SA&A) process for their information systems. The ISSO typically performs this function for the system owner for the information system. The PIA is included as one of the artifacts in the Security Assessment and Authorization package. Responsibilities include, but are not limited to the following:

- a. Following any of the scenarios that would trigger the need for a PIA, the ISSO will draft a new PIA or modify a PIA and coordinate with the System Owner and CRA.
- b. If assistance is needed that cannot be obtain in either HHS or CMS PIA guidance documentation, the ISSO will contact the CRA to coordinate with the Privacy Advisor for additional assistance.
- c. Cooperatively engage with the system owner, CRA, Privacy Advisor and leadership to ensure any additional comments and suggestions are included in the PIA as needed.
- d. Assist in identifying and remediating potential privacy risks; notify System/Business owners of the PIA requirement;
- e. Inform the CRA when a planned, new or existing system will require a PIA.

5. Privacy Impact Assessment Workflow

At CMS, the tool for completing the PIA is CMS FISMA Controls Tracking System (CFACTS). When going through the questions in the PIA, it is advised to review the CMS help text guidance built into CFACTS as well as the HHS PIA writers’ handbook available on the front page for each question. The procedures in the table below gives a summary review of the actions necessary to complete a new PIA or modify an existing PIA.

Step	Actions
1. System/Business Owner/ISSO/CRA	Following any of the scenarios that would trigger the need for a PIA as described in section 3, the System/Business Owner or ISSO drafts a new or revised PIA in CFACTS and contacts the CRA upon completion. In CFACTS, the queue for the System/Business owner or ISSO is “ISSO Submitter” for the PIA.

Step	Actions
2. CRA/Privacy Advisor	<p>The CRA reviews the PIA in collaboration with the Privacy Advisor and coordinates recommended changes with the system/business owner or ISSO. Any identified privacy risks or compliance issues should be resolved before submission to the SOP for approval.</p> <p>If the SOP or SAOP recommends changes, the review process will continue from this step as needed until the PIA is approved and finalized by the SAOP.</p>
3. SOP/Final Approver	<p>The SOP or designated Final Approver will review the PIA and recommend approval to HHS if no changes are recommended.</p>
4. SAOP	<p>The SAOP will designate staff to review all PIAs before approval for signature. If no changes are recommended, the SOP and SAOP will digitally sign the PIA. Once signed by the SOP and SAOP, the PIA is approved and complete for a length of time as discussed in section 2.</p>
5. SAOP	<p>HHS will submit the final PIA for publication to the HHS PIA internet site at https://www.hhs.gov/pia</p>

6. Question-by-Question guidance and resources

There is guidance available which is designed to help authors and reviewers complete each question in the PIA template. Before starting the HHS PIA template in CFACTS, it is recommended to have the following guidance available:

- The HHS PIA and PTA Writers’ Handbook designed to help authors and reviewers complete the PIA/PTA questions in accordance to what HHS standards. The Handbook is titled “[PIA and PTA Writers Handbook](#)” on the CFACTS front page and available as needed from the CRA and Privacy Advisor.
- CMS guidance further explains what HHS is looking for each question in the PIA. Also included in the CMS guidance is template language in the event the information system contains only access credentials; however, the language can also be borrowed if it fits with the information system. The document is titled “[CMS PIA Guidance](#)” on the front page in CFACTS. The same content in the CMS guidance document is also built into CFACTS help text for each question in the PIA.
- The Privacy Handbook is guidance intended for CMS Business Owners and Project Managers who need to collect, use, and disclose personally identifiable information (PII), including protected health information (PHI). If there is a possibility that other documentation is required such as a Computer Matching Agreement, Information

Exchange Agreements or a System or Records Notice the Privacy Handbook is an excellent resource.

Additional program and system documentation may be available to assist in the completion of the PIA and may provide reusable language to respond to some of the questions in which Appendix B provides more information. If you require additional assistance not available in the guidance, please reach out to your CRA and/ or Privacy Advisor for questions.

7. Third-Party Websites and Applications (TPWA)

TPWA uses include technologies such as social media websites or applications that CMS uses to communicate with and engage the public for program purposes and for implementing principles of the Open Government Directive. OMB defines TPWAs as “web-based technologies that are not exclusively operated or controlled by a government entity, or web-based technologies that involve significant participation of a nongovernment entity. Often these technologies are located on a ‘.com’ website or location that is not part of an official government domain. However, third-party applications can also be embedded or incorporated on an agency’s official website.

As use of TPWAs expands, federal agencies are required to take specific steps to protect individual privacy whenever they use TPWAs to engage with the public (e.g., LinkedIn, Twitter, Flickr, Facebook, Instagram, blog/microblogging tools, YouTube, etc.)

Under OMB directive and HHS policy, CMS must conduct a PIA for each such use of a TPWA⁶. The purposes of the TPWA, and the procedures and responsibilities mirror those of the standard PIA described throughout this document.

When using a TPWA, the relevant CMS program management, system/business owner, or ISSO responsible for completing the PIA should adhere to the following requirements:

- Contact the CRA and Privacy Advisor for guidance and materials as needed
- Examine the third party’s privacy policy to evaluate the risks and determine whether the website or application is appropriate for CMS’s use;
- Prepare a TPWA PIA when the public will be engaging with the CMS using a TPWA. That is, TPWAs that do not interact with the public do not require the completion of a TPWA PIA. Tools used for internal administration do not need a TPWA PIA, but are still subject to other listed standards and policies;
- Use an external link notice when visitors are directed to a nongovernment website;
- Review CMS’s web privacy policy (on CMS.gov) and contact the SOP as needed to ensure the TPWA use is appropriate and/or that the Agency policy is accurate in view of the TPWA use; and
- Prominently post a Privacy Notice on the third-party website or application itself, to the extent feasible. Required elements of the Privacy Notice are set out in OMB M-10-23, Guidance for Agency Use of Third-Party Websites and Applications (June 25, 2010).

⁶ TPWA PIAs are different from the standard PIA with contain different questions; please consult with the CRA or Privacy Advisor for a template if needed. TPWA PIAs still follow the review and renewal guidelines as standard PIAs outlined in this document with the exception that they do not expire at a set period.

Notice requirements are further described in HHS Memorandum: Implementation of OMB M-10-22 and M-10-23 and the HHS-OCIO Policy for Information Systems Security and Privacy.

Appendix A: Tips for Writing an Effective PIA

- ✓ Answer briefly; text fields have a limited capacity when translated to the final documentation.
- ✓ Write in a way that is easily understood by the general public; avoid using overly technical language, clearly define technical terms and references if needed to describe system.
- ✓ Define each acronym the first time it is used; use the acronym alone in all subsequent references.
- ✓ Do not include sensitive/confidential information or information that could allow a potential threat source to gain unauthorized access into the system (e.g., do not provide detailed information on technical security controls).
- ✓ Provide information about authentication credentials. We need to know if the system is accessed using system-specific logon information such as a username and password. This would not be the case if, for example, the system was subject to authentication using only PIV access and single sign-on authentication, because in that case user credentials are stored outside the system boundary. Please include a statement indicating whether logon information is in the system.
- ✓ Make it clear who the “users” are. In some cases, it may be confusing whether “users” refers to individuals who are creating records about themselves, or whether “users” are CMS staff members receiving and acting on this information. Please make this distinction clear the first time the term “users” is used.
- ✓ Verify whether the system needs an Information Collection Approval number from OMB. Depending how you answer Question 23, Question 23a will appear. It asks about an OMB Information Collection Approval number. Under the Paperwork Reduction Act (PRA), the POC/system owner may need to obtain an information collection approval number from the White House Office of Management and Budget. Use the information in the CMS guidance and HHS PIA writers’ handbook regarding this question to contact PRA subject matter experts as needed.
- ✓ System of Records Notice (SORN). Questions 22 and 22a are relevant to SORNs. If the system uses PII to retrieve records, it may need to be covered by a SORN. Any system that has already received Privacy Office signatures should already reference a SORN. If not, you may need to seek guidance from ISPG or DSPPG to determine whether a SORN is required and in identifying an existing SORN that might apply.
- ✓ Authority to Collect. Question 21 asks for the legal authorities governing information collection. Every system with PII must have an authority to collect this information. This will be a statute or Executive Order that either (a) permits or requires collection of the PII, or (b) permits or requires the underlying activity, for which it is necessary to collect PII.
- ✓ Retention schedule. Question 37 asks about the system retention schedule. Every system (whether it contains PII or not) should have been made subject to an information retention schedule. Check with Records Officer to identify the appropriate retention schedule.

Appendix B: Additional Guidance & Resources

There may be some existing documentation for the information system, which would make it possible to reuse language to respond to some of the questions in the PIA. Below are some additional resources that is recommended to review before beginning the PIA and to have on hand while preparing the PIA includes:

- Some information systems have web sites and/or online applications which further explain the relevant programs that are supported by the system;
- Information Collection Requests (ICRs) can be a resource for information on the system if it collects information from the public and is subject to the Paperwork Reduction Act (PRA);
- Privacy Act Notice Statements and System of Records Notices (SORNs) is an important resource for some of the questions in the PIA if the system is subject to the Privacy Act.
- Privacy policies are a resource for the PIA if the system uses one or more web sites that are subject to OMB M-10-22 and OMB 10-23.
- Lifecycle Artifacts such as the System Security Plan (SSP), which would include privacy controls as well.
- For information on the National Institute of Science and Technology (NIST) 800-53 Privacy Controls and the relation to questions in the PIA, section III of the CMS PIA Guidance provides a suggested cross reference.

Appendix C: References

- Privacy Act of 1974, as amended, 5 U.S.C. 552a, Pub .L. 93-579
- E-Government Act of 2002, Section 208, Pub. L. 107-347
- Federal Information Security Modernization Act (FISMA) of 2014, Pub. L. 113-283, 128 Stat. 3073
- OMB M -05-08, Designation of Senior Agency Official for Privacy
- Circular A-130, Managing Information as a Strategic Resource
- OMB M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies
- OMB M-10-23, Guidance for Agency Use of Third-Party Websites and Applications.
- OMB M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government of 2002
- The Paperwork Reduction Act of 1995 (PRA)
- CMS Information Systems Security and Privacy Policy (IS2P2)
- NARA (44 U.S.C. Chapter 21)
- HHS Privacy Impact Assessment Program Policy (2019)