The U.S. Department of Housing and Urban Development (HUD)

PRIVACY COMPLIANCE PROGRAM PLAN

January 2022

Document Change History

Issue	Date	Description
Version 1.0	03/30/2020	Establishes HUD's Privacy Compliance Program Plan policies and procedures for all HUD personnel to maintain compliance.
Version 1.1	01/30/2022	Added Privacy Handbook compliance requirements.

Contents

1. Introduction

The U.S. Department of Housing and Urban Development's (HUD) Privacy Program mission is to protect and minimize impacts on the privacy of individuals, while achieving HUD's mission. The purpose of the HUD Privacy Compliance Program Plan is to commensurate authority to enforce implementation of policy and procedures. The Plan enables compliance with HUD Privacy Program requirements, including federal requirements and the full suite of HUD Privacy policies, guidance, directives, and memorandums.

The HUD Privacy Program implements requirements of the Privacy Act of 1974, as amended; E-Government Act of 2002; and the Federal Information Security Modernization Act (FISMA), as well as policy directives and best practices issued in furtherance of those Acts. The HUD Privacy Office oversees and operates the Privacy Program including: Privacy stakeholder roles and responsibilities, Personally Identifiable Information (PII) handling, PII Protection at Workstations Policy, Annual Federal Reporting, System of Record Notice, Privacy Impact Assessments, and Record Retention Policies. This document includes relevant requirements from those processes to enable compliance.

This Privacy Compliance Program Plan is a living document, intended to enable compliance by listing the relevant requirements from the suite of HUD Privacy policies and procedures. This document outlines information needed to comply with HUD Privacy standards, including stakeholder's roles & responsibilities, policies & procedures, and Federal reporting requirements. Each section in this plan will note which offices and personnel are subject to the requirements. The Privacy Compliance Program Plan has commensurate authority to enforce implementation of policy and procedures. For full guidance and details, refer to the source policies and guidance documents via the links provided in each section.

2. Annual Update

The Privacy Compliance Program Plan will be reviewed at minimum on an annual basis to ensure the policies, procedures, and requirements needed for compliance with Federal and HUD Privacy are included. It is the CPO's responsibility to ensure that this document is reviewed and updated annually. Notice regarding material changes to this plan will be communicated by the HUD Privacy Office.

3. Penalties for Non-Compliance

Privacy Liaison Officers (PLOs) are responsible for reporting on Compliance Program Plan status and violations to the HUD Privacy Office on a continual basis. Some individual privacy policies have additional compliance measures, which are noted in each respective section.

4. Stakeholder Roles and Responsibilities

This section outlines the HUD's Privacy roles and their respective responsibilities, including channels of communication between roles and role-specific training requirements.

4.1 Senior Agency Official for Privacy

Stakeholder Description: In accordance with the Office of Management and Budget (OMB) Memorandum 16-24, the Senior Agency Official for Privacy (SAOP) has agency-wide responsibility and accountability for developing, implementing, and maintaining an agency-wide privacy program to ensure compliance with all applicable statutes, regulations, and policies regarding the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII by programs and information systems, developing and evaluating privacy policy, and managing privacy risks at the agency. The SAOP is responsible for:

- Serving as HUD's senior policy authority on matters relating to the public disclosure of information, advising on privacy issues related to informed consent, disclosure risks, and data sharing;
- Developing and overseeing implementation of agency-wide policies and procedures relating to the Privacy Act, and assuring that personal information contained in Privacy Act systems of records is handled in compliance with its provisions;
- Complying with Privacy Act requirements for publishing, revising, and rescinding System of Record Notices (SORNs) as needed;
- Communicating HUD's privacy vision, principles, and policies internally and externally working with the Privacy Liaison Officers (PLO's) in each business area as appropriate;
- Advocating strategies for data and information collection and dissemination, and conducting an annual PII inventory to ensure HUD's privacy policies and principles are reflected in all operations;
- Managing privacy risks associated with HUD activities that involve the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII by programs and information systems;
- Ensuring that HUD employees have the appropriate training and education concerning privacy laws, regulations, policies, and procedures;
- Working with HUD stakeholders to ensure the vendors with access to PII that engage in business with HUD abide by federal privacy requirements;
- Overseeing HUD's process for reviewing and approving Privacy Impact Assessments (PIA) to ensure compliance with the E-Government Act;
- Coordinating with HUD's Chief Technology Officer (CTO) and Chief Information Security Officer (CISO) to ensure that the FISMA authorization and accreditation (A&A) process for new and existing systems appropriately addresses privacy-related risks;

- Partnering with the CTO and CISO to ensure all aspects of HUD's privacy program are incorporated into HUD's enterprise infrastructure, information technology (IT), and IT security program;
- Ensuring HUD is compliant and up to date with federal reporting and publication requirements and deadlines.

4.2 Chief HUD Privacy Officer

Stakeholder Description: The Chief HUD Privacy Officer (CPO) is responsible for substantive components of HUD's Privacy Office, as well as reviewing and updating this document annually. In accordance with OMB Memorandum 16-24, HUD's SAOP has delegated the daily operations of HUD's privacy program to the CPO. Responsibilities and requirements include:

- Overseeing privacy team staff, including analysts and specialists;
- Developing and overseeing implementation of agency-wide policies and procedures relating to the Privacy Act, and assuring that personal information contained in Privacy Act systems of records is handled in compliance with its provisions;
- Complying with Privacy Act requirements for publishing, revising, and rescinding System of Record Notices (SORNs) as needed;
- Communicating HUD's privacy vision, principles, and policies internally and externally working with the Privacy Liaison Officers (PLO's) in each business area as appropriate;
- Ensuring that HUD employees have the appropriate training and education concerning privacy laws, regulations, policies, and procedures;
- Regularly reviewing and ensuring all privacy related policies and guidance are current and compliant with Federal standards;
- Managing day to day operations of the HUD Privacy Office;
- Overseeing HUD's process for reviewing and approving PIAs submitted by PLOs;
- Reviewing and tracking SORNs submitted by PLOs for HUD Offices;
- Consulting with HUD Offices to ensure implementation of and compliance with Privacy policies;
- Managing the PLO program, including working with PLOs to maintain agency-wide compliance with privacy regulations and up to date federal reporting.
- Implementing and overseeing incident response procedures and reporting breaches to the SAOP.

4.3 Privacy Liaison Officers

Stakeholder Description: In accordance with OMB Memorandum 16-24, the SAOP has delegated authority to the CPO to assign roles needed for privacy compliance. The CPO has established that every business area must appoint a Privacy Liaison Officer (PLO) who serves as the liaison between their respective Offices and the HUD Privacy Office. The PLO plays a critical role in supporting the HUD Privacy Office's mission to protect and minimize impacts on the privacy of individuals. PLOs serve as the ambassador between your Office and the HUD Privacy Office. The PLOs responsibilities include:

- Compliance: Enabling HUD to demonstrate compliance with privacy legislation and reduce privacy risk.
    - Overseeing compliance with privacy regulations in their respective business area, including understanding PIAs, SORNs, CMAs**,** breach notification guidelines, and other requirements for handling PII which is later detailed in this document;
    - Serving as a resource for conducting essential functions in their respective office, such as PIAs, SORNs, and CMAs;
    - Signing off as the Privacy representative for their Program / Field Office;
- Champion: Clearly articulating policies, procedures, and guidelines that are meaningful and easily accessible for the business area.
    - PLOs are responsible for understanding the relationship between their Office's business needs / functions and the relevant privacy policies, procedures, and best practices;
    - Helping their Office understand their privacy responsibilities and support them in carrying out these essential functions;
    - Ensuring their Office understands what PII is, can identify repositories, and is aware of retention requirements;
- Contact: Providing point of contact for individuals to escalate privacy related inquiries;
    - Being the voice of the HUD Privacy Office for the Program / Field Office, sharing updates and best practices – as well as being the escalation point in case of any questions or in the event of an incident;
    - Being the voice of the Office to the HUD Privacy Office and PLO community – sharing best practices, common challenges, and ideas for making HUD a proactive privacy player;
- Attending monthly PLO meetings;
- Participating in annual PII inventory and assisting in conducting an annual risk assessment;
- Providing input to HUD Privacy Office on project priorities;
- Providing feedback to Privacy and Divisional Information Security, including in the event of incidents;

- Ensuring all personnel within their Office are notified and aware of HUD Privacy Office Directives, Memorandums, and other requirements;
- Distributing Privacy guidance materials and documents to HUD employees and contractor within their Office as directed by the HUD Privacy Office (i.e. Privacy Act exceptions guidance);
- Tracking and reporting Privacy violations and non-compliance to the HUD Privacy Office;
- Attending required role-based trainings which include operational security concerns regarding document storage twice a year.

5. HUD Privacy Role-Based Training

All HUD employees and contractors are required to take annual privacy training. In addition to the annual training, some employees are required to complete additional role-based training.

Description: Starting FY20, the HUD Privacy Training Plan informs HUD personnel and contractors of Privacy-related policies, procedures, and required actions for compliance. Privacy training topics will be integrated into HUD's enterprise-wide, General Cybersecurity Awareness Training (GCAT) via web-based training, ensuring all personnel and contractors are aware of Privacy policies, mandatory procedures, best practices, and compliance requirements. See the HUD Privacy Training Plan for detailed requirements.

Compliance Requirements:

- **All HUD Employees, Contractors, and Third parties with access to HUD information systems and data** must attend privacy awareness training and must recognize what is and isn't classified as PII and understand requirements and best practices for complying with HUD and federal privacy requirements.
- The **CPO** is responsible for providing PLOs with semi-annual training on HUD Privacy policies and guidance, including PIA and SORN requirements, PII handling requirements, Privacy Act exceptions guidance, and breach notification guidelines.
- **PLOs** are responsible for attending semi-annual PLO trainings and ensuring their Office is in compliance with HUD privacy policies and guidance.
- **All Manager/Supervisor level personnel** need to attend training on: how to properly handle PII at their access level; privacy risks associated with authorizing access to other personnel; importance of only authorizing access to personnel with relevant duties; and regularly auditing access provided to team members.
- **HUD Employees and Contractors with elevated access privileges** must attend trainings on PII handling requirements and best practices, based on the role's needs and access.

- The HUD Privacy Office is responsible for conducting annual reviews of the HUD Privacy Training Plan and making updates as necessary.

Additional Authority & Non-Compliance Procedures: Elevated access privileges will be revoked until HUD employees or contractors are compliant with role-specific training requirements.

6. Policies & Procedures

This section includes an overview of HUD's Privacy policies and procedures, with information on their respective compliance requirements and links to the source documents.

7. PII Protection at Workstations Policy

Description: The PII Protection at Workstations Policy covers the responsibilities of personnel regarding the protection of information assets in the physical workspace. Privacy risks exist in both digital and physical handling, and protections are needed to prevent unauthorized access and disclosure of PII. The policy serves to improve confidentiality and management of risks, create a more professional workspace, improve cleanliness of the working environment, and improve management of filing and data.

Compliance Requirements:

- **PLOs** must ensure that copies of the PII Protection at Workstations Policy are posted in visible locations in the office workspace.
- **PLOs** must ensure that personnel are provided with access to the PII Coversheet described in the PII Protection at Workstations Policy.
- **PLOs** must coordinate with **Managers** to oversee adherence to the policy by periodically conducting an office walkthrough, checking workstations for policy violations, and reporting the Office's physical security measures twice per calendar year to the HUD Privacy Office.
- **All HUD Employees and Contractors** must abide by the practices set forth in the PII Protection at Workstations Policy

Additional Authority & Non-Compliance Procedures:

- The **CPO** is responsible for reviewing incidents of non-compliance and taking steps to follow-up with PLOs to ensure personnel comply with the PII Protection at Workstations Policy. The **CPO** will escalate repeated non-compliance to the **SAOP**.
- The **CPO** is responsible for sending notice to **PLOs** for failure to report on or enforce their physical security efforts, with this being escalated to their supervisor as a next step.

8. Privacy Program Plan

Description: The HUD Privacy Program Plan provides an overview of the strategic goals and objectives of HUD's Privacy Program. It includes a description of the Privacy Program's structure, the responsibilities of privacy staff, and the resources dedicated to accomplishing the Privacy Program's goals.

Compliance Requirements:

- The **Privacy Office** must review and update the Privacy Program Plan on an annual basis.

9. HUD Privacy Handbook

Description: The HUD Privacy Handbook establishes a set of privacy principles that govern how to handle Personally Identifiable Information and explains how HUD complies with Federal privacy requirements. It serves to minimize risk of PII compromise and offer guidance on proper PII safeguards, such as encryption, limits on information use, and storage device management. Additionally, the Privacy Handbook emphasizes the PII Handling requirements outlined in the HUD Privacy Policy. It establishes the PII handling protocol that all HUD personnel must follow.

Compliance Requirements:

- **PLOs** must ensure that all HUD personnel review the HUD Privacy Policy and have thethe link to where the document can be found online.
- **All HUD personnel involved in the processing of PII** must understand and comply with the requirements set forth in this policy.
- **Managers** are responsible for their employees' understanding of privacy protection requirements and the penalties for non-compliance.
- **Managers** must notify **PLOs** of any Privacy Policy violations and noncompliance.
- **PLOs** are responsible for tracking violations of the Privacy Policy and reporting them to the HUD Privacy Office.
- **All HUD personnel involved in the processing of PII** must understand and comply with the requirements set forth in this policy.
- The **HUD Privacy Office** is responsible for substantively updating the Privacy Handbook as needed.
    - The **HUD Privacy Office** is responsible for checking and updating all links in the Handbook no less than twice annually.
    - The **HUD Privacy Office** is responsible for ensuring the updated version of the Privacy Handbook is available on the HUD Privacy Website.

Additional Authority & Non-Compliance Procedures:

- Noncompliance will result in reports to the PLO and possible escalation to the **Privacy Office** and **CPO**.
- The **CPO** is responsible for reviewing incidents of non-compliance and taking steps to follow-up with PLOs to ensure personnel comply with the PII Handling Directive. The **CPO** will escalate repeated non-compliance to the **SAOP**.

10. Privacy Act Disclosures Procedures

Description: The HUD Privacy Act Disclosures Procedures describes process for recording and handling disclosures of Privacy Act Information. The PLOs are responsible for handling all Privacy Act requests in their respective Offices, including tracking progress, coordinating with the HUD Privacy Office throughout, and accounting of disclosures in accordance with federal and HUD requirements. The Privacy Act requires agencies keep accurate accounts of when and to whom personal records are disclosed. These accounts should include information on the date and nature of the disclosure as well as information on the recipient.

Compliance Requirements:

- **PLOs** must ensure that all HUD personnel involved with handling Privacy Act requests are provided with a digital copy of the Privacy Act Disclosures Procedures and the link to where the document can be found online.
- **All HUD personnel involved with handling Privacy Act requests** must comply with the procedures and record keeping requirements.

11. Privacy Incident Response Procedures

Description: OMB 16-24 requires all individuals with access to the agency's Federal information and information systems to report a suspected or confirmed breach to the agency as soon as possible and without unreasonable delay, consistent with the agency's incident management policy and procedures, NIST standards and guidelines, as well as US-CERT notification guidelines. This includes a breach in any medium or form, including paper, oral, andelectronic. See the HUD Breach Notification Response Guide (HBNRP) for detailed incident response procedures and definitions.

Compliance Requirements:

- The **SAOP** is responsible for assessing privacy breaches and determining subsequent actions consistent with Federal guidance and the HUD PIRP.
- The **CPO** is responsible for assessing and communicating privacy breaches to the SAOP.
- **PLOs** are responsible for reporting privacy incidents in a manner consistent with Federal guidance and the HUD PIRP.

- **System Owners** are responsible for coordinating with PLOs to report privacy incidents in a manner consistent with Federal guidance and the HUD PIRP.

12. Maintenance of Central Collaboration Area

Description: HUD's public-facing Privacy Website serves as a repository and central collaboration area for HUD Privacy Program policies, procedures, and guidance. The website serves to include current privacy program policies, procedures, guidance, and templates. HUD personnel should consult this page when searching for templates and materials needed for Privacy-related tasks. The HUD Privacy SharePoint site serves as a repository of all HUD Privacy materials, including HUD Privacy Office resources that cannot be shared with the public.

Compliance Requirements:

- The **HUD Privacy Office** is responsible for maintaining and updating the HUD Privacy Website central collaboration area as well as the HUD Privacy SharePoint repository. They should be reviewed and updated at least once per quarter.
- **All HUD personnel** should refer to the central collaboration area for resources needed for privacy related responsibilities.

13. Communications Plan

Description: The HUD Privacy Office Communications Plan outlines (1) the process for developing and executing communications across HUD, (2) the available messaging channels for distributing communications, and **(**3) the key stakeholders in support of the HUD Privacy Office's mission to minimize negative impact of the privacy of individuals and to build a strong culture of privacy protection based on enforcing sound privacy practices in compliance with applicable laws to maintain public trust.

Compliance Requirements:

- The **CPO** is responsible for communicating:
  - **Quarterly Executive Leadership Meeting** which informs executive leadership on key privacy efforts, highlights, projects, and risks.
  - **HUD Privacy Office Directives and Memos** (as needed) which formally communicates agency-wide privacy policy updates, guidance, requirements, deadlines and required personnel actions.
- The HUD Privacy Office is responsible for communicating:
  - The Executive Leadership Dashboard (bi-monthly) which provides status updates on HUD Privacy Office strategic priorities, policies, process updates, and information on Privacy incidents.
  - Privacy Liaison Officer Meeting (monthly) which communicates key Privacy Policy and procedure updates, guidance, requirements, expectations, timelines, need-to-know topics, and key Privacy efforts and projects.

14. PII Minimization Plan

Description: The HUD PII Minimization Plan details priorities, strategy, and implementation mechanisms for PII identification and minimization. The HUD Privacy Office prioritizes eliminating the collection of unauthorized or unnecessary PII as a foundation for a robust Privacy Program. PII identification and minimization will be achieved through prioritization of: creating inventories of HUD's PIAs, SORNs, and PII, including procedures, timelines, and compliance mechanisms to ensure their maintenance; annual HUD-wide Privacy Data Questionnaires; and ongoing training and awareness campaigns.

Compliance Requirements:

- The **PLO** is responsible providing input on PIAs, SORNs, and PII to the **HUD Privacy Office**.
- The **HUD Privacy Office** is responsible for conducting annual HUD-wide data calls.
- The **HUD Privacy Office** is responsible for ensuring maintenance of inventories through annual reviews

15. PII Inventory Maintenance & Compliance Directive

Description: The Privacy Office Directive 02-00, PII Inventory Maintenance & Compliance (2020) establishes compliance measures to ensure completion and maintenance of HUD's PII Inventory, as required by the Federal Information Modernization Act of 2014 (FISMA). The Directive applies to the HUD PLOs and System Owners to provide timely research and feedback in their respective Offices to the Privacy Office to ensure completion and maintenance of the PII Inventory.

Compliance Requirements:

- The **PLO** is responsible for reporting on their respective Office's PII holdings at least annually in a manner that is accurate, relevant, timely, and complete. This will be supported by HUD Program Offices ensuring that PII holdings within system of records, whether in electronic or nonelectronic form, is kept the minimum necessary for the proper performance of agency functions. Noncompliance will result in reports to the PLO and possible escalation to the **CPO.**
- The **PLO** is responsible for tracking violations and misuse of any information contrary to the terms of a SORN or PIA and reporting them to the Privacy Office.
- The **CPO** is responsible for leading an annual review in which PLOs are required to report on their Office's complete PII holdings, including progress of PII minimization efforts and compliance with retention schedules.
- The **SAOP** and **CPO** has executive oversight and is responsible for ensuring the PII Inventory is reviewed and maintained annually

- **System Owners** are required to coordinate with the PLOs of their respective office to ensure SORNs and PIAs are submitted on time and must also provide any information needed for annual PII Inventory review.

16. Systems of Records Accounting Requirements

17. Privacy Impact Assessment

Description: A Privacy Impact Assessment (PIA) is an analysis of how information in identifiable form is collected, maintain, stored, and disseminated, in addition to examining and evaluating the privacy risks and the protections and processes for handling information to mitigate those privacy risks. A PIA is required when HUD develops, procures, or uses information technology to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII. PIAs include information on who has access to PII and what controls are in place to protect the information.

Compliance Requirements:

- **All HUD Information Systems** and **Electronic Collections** are required to have a PIA, in the current template.
- **PLOs** are responsible for submitting PIAs using the current template. The PIA Reference Guide provides detailed instructions for completing a PIA.
- **PLOs** are responsible for sending completed PIAs to the HUD Privacy Office.
- **All System Owners** must cooperate with PLOs to collect necessary information for each respective system's PIA.

18. System of Records Notices

Description: Each System of Records Notice (SORN) describes what, why and how HUD collects, maintains, uses and disseminates records in the system. Some systems maintain information on HUD employees while others maintain information from or about individuals outside of HUD. These Government-wide systems are maintained by other Federal agencies that hold some of the operating authority over the records such as the Office of Personnel Management's Employee Performance File system.

Compliance Requirements:

- **All HUD Information Systems** that contain a group of records from which information is retrieved by the name of an individual, or by any number, symbol, or other unique identifier assigned to that individual are required to have a SORN.
- **PLOs** are responsible for ensuring SORNs describing each system of records be published in the Federal Register for review and comment by the public and other interested parties as part of the prescribed review and approval process.
- **System Owners** are required to provide necessary information to PLOs for proper filing of notices.

- The **HUD Privacy Office** is responsible for submitting SORNs to the Federal Register for publication.

19. Computer Matching Agreements

Description: All Computer Matching Programs must have requisite Computer Matching Agreements. A Computer Matching Agreement (CMA) is a written agreement between the source agency and the recipient agency (or non-Federal agency) specifying the terms of a matching program. There are four categories of matching agreement: new, extension, modification, and re-establishment.

Compliance Requirements:

- **PLOs** are responsible for ensuring CMAs are filed and renewed on a timely basis for all systems of records within their respective offices that are used in matching programs. This includes tracking dates and deadlines of establishment, extension, and renewal.
- **PLOs** must track and report all violations of any CMA terms pertaining to systems of records within their office.
- **System Owners** in each office are responsible for cooperating with the PLO to track compliance and renewal of CMAs.
- **System Owners** are responsible for providing PLOs with all necessary information to file Computer Matching Agreements.
- The **HUD Privacy Office** is responsible for submitting CMAs to the Federal Register for publication and submitting all required documents to the OMB and Congress.

20. Federal Reporting

This section of the Privacy Compliance Plan covers compliance requirements to ensure HUD meets Federal privacy reporting mandates.

21. Annual CMA Activity Report

Description: Per Office of Management and Budget (OMB) federal reporting requirements, HUD must submit an Annual Computer Matching Agreement (CMA) Activity Report that accounts for all matching programs HUD engaged in during the reporting year. The report must include a list of all CMAs that HUD participated in during the reporting year.

Compliance Requirements:

- The **SAOP** and **CPO** are responsible for ensuring the annual CMA Activity Report is completed and filed.

- The **Privacy Office** is responsible for consolidating information and submitting the activity report.
- **PLO**s are responsible for collecting information needed for the Activity Report from their respective Offices.
- **All HUD System Owners** are required to cooperate with PLOs to produce required documentation.

22. Annual SAOP FISMA Report

Description: The Annual SAOP FISMA Report Reference Guide provides instructions and timetables for completing the Annual SAOP FISMA Report. Each year, the SAOP must review the administration of the agency's privacy program and report compliance data to OMB. The SAOP and HUD Privacy Office must: (1) Confirm report requirements and deadlines, (2) Collect required information, (3) Prepare the draft report, (4) Review and submit the final report via CyberScope. The following sections detail the documents and data to be submitted, roles and responsibilities for collecting these artifacts, and timeline for their collection.

Compliance Requirements:

- The **SAOP** is responsible for drafting and submitting the Annual SAOP FISMA Report.
- The **HUD Privacy Office** is responsible for checking annual OMB guidance regarding metrics and reporting deadlines and compiling necessary documentation from PLOs for the report.
- **PLOs** are responsible for overseeing their Offices to ensure information needed for compiling the final report is maintained, consolidated, and provided to the HUD Privacy Office for timely review and submission.
- **Individual System Owners** are required to cooperate with PLOs in collecting necessary information for the SAOP report.

23. Incident Reporting

Description: FISMA requires agencies to report privacy incidents to the OMB on a monthly basis. Breaches that qualify as major incidents must be reported to Congress within 7 days of identification. The HUD Breach Notification Response Plan (HBNRP) provides detailed instructions for reporting incidents.

Compliance Requirements:

- The **SAOP** is responsible for coordinating with the Chief Information Officer (CIO) to determine if a breach constitutes a major incident.
    - If a breach constitutes a major incident, the **SAOP** is responsible for submitting this information to the agency head and ensuring the breach is reported to Congress within 7 days of identification.

- The **CPO** is responsible for informing the SAOP of all moderate and major incidents.
- **System Owners** are required to cooperate with the Privacy Office to collect details regarding privacy incidents for incident response, recovery, and notification procedures.