

OFFICE OF EVALUATION OPEN RECOMMENDATIONS

REPORT NUMBER	REPORT DATE	REC #	RECOMMENDATION TEXT
2013-ITED-0001	11/29/2013	32	Train personnel on encryption solutions available to those users handling PII and sensitive information
2013-ITED-0001	11/29/2013	36	REPEAT FINDING: Review business impact assessments of HUD applications and consolidate them into an entity-wide business impact assessment as described in FISMA standards. Recommendation 1C, 2012-DP-000
2013-ITED-0001	11/29/2013	51	Formally confirm / appoint Privacy Points of Contact in each Program Office and Regional Office
2013-ITED-0001	11/29/2013	56	Implement a compliance program (through the OCIO) and hold program offices accountable for implementing IT security requirements
2014-ITED-0001	4/30/2014	4	Issue a privacy directive outlining an organizational approach to proper handling of PII, to include establishing accountability of managers for their employees' understanding of privacy protection requirements and the penalties for non-compliance
2014-ITED-0001	4/30/2014	7	Issue a formal directive requiring timely research and feedback by the Program Offices to the Privacy Office to ensure completion of the PII inventory; hold managers accountable for timely response by their office
2014-ITED-0001	4/30/2014	8	Develop or procure, and implement, a solution that enables scanning and detection of PII on any and all network and computer resources
2014-ITED-0001	4/30/2014	10	Update and issue Incident Response and Reporting policies and procedures, including privacy breach response standard operating procedures
2014-ITED-0001	4/30/2014	11	Align the DLP solution management within existing continuous monitoring processes
2014-ITED-0001	4/30/2014	17	Conduct a quality review and update of all SORN data in CSAM; establish procedures and assign responsibilities to ensure data is properly maintained
2014-ITED-0001	4/30/2014	18	Complete the ongoing project to review and update existing IPAs and PIAs, including a master reconciliation between system inventory, PIAs and SORNs; prioritize all PIAs that were completed on an outdated PIA template
2014-ITED-0001	4/30/2014	21	Establish a repeatable process, including a master repository, to ensure collection and maintenance of accurate PII inventory data
2014-ITED-0001	4/30/2014	32	Conduct a risk assessment of physical security measures in place at HUD in order to determine HUD's current physical security posture, identify its vulnerabilities, and implement safeguards to mitigate risk.
2014-OE-0002	2/12/2016	2	We recommend that the Deputy Secretary strengthen DEC's authority to enforce program requirements. Program offices should be directed to incorporate risk management procedures, to include risk-based, data-driven referrals to DEC, and implement a process that allows DEC to recommend enforcement actions independently. The Deputy Secretary or designee should be the final arbiter when disagreements arise.
2014-OE-0002	2/12/2016	4	We recommend that the Deputy Secretary direct program offices and REAC to collaborate with DEC to research the types of data that would provide clear indications of financial and physical performance failures appropriate for use in data-driven referrals to DEC from each program office.

2014-OE-0003	11/14/2014	4	Further develop configuration management program policy to include enterprise automated deviation handling and deviation risk mitigation processes
2014-OE-0003	11/14/2014	8	Complete and maintain an accurate inventory of HUD information systems, to include General Support Systems (GSS), major applications, and minor applications, and ensure Minor Applications are documented within GSS or major application systems
2014-OE-0003	11/14/2014	13	Incorporate contractor personnel and facilities into enterprise contingency planning
2014-OE-0003	11/14/2014	14	OCPO in conjunction with OCIO need to establish policies and procedures for implementing contractor oversight requirements to assure ongoing compliance with FISMA security requirements
2014-OE-0003	11/14/2014	17	Develop a long term strategic plan for managing the IT portfolio; direct additional emphasis towards legacy applications with imminent risk
2015-OE-0001	11/19/2015	1	Finalize the implementation of automated tools from the DHS CDM program and develop a plan or roadmap to maintain those tools and processes to facilitate an enterprise-wide continuous monitoring program. [Note: this recommendation replaces FY 2014 recommendation 3] [continuous monitoring
2015-OE-0001	11/19/2015	3	Document complete policy and procedures for identity and access management at all levels, including specific systems and applications. Ensure such policy and procedures are properly documented and maintained within security documentation that is maintained in CSAM. [identity and access management
2015-OE-0001	11/19/2015	4	Ensure completion of the current FICAM initiative to automate portions of the personnel on- and offboarding process. [identity and access management
2015-OE-0001	11/19/2015	5	Develop procedures for and resource the DLP [data loss prevention] solution to properly utilize the capability of identifying and preventing PII [personally identifiable information] from being released outside the agency. [incident response
2015-OE-0001	11/19/2015	6	Develop procedures and capabilities for incident analysis, correlation and analysis, as prescribed by NIST SP 800-61, Revision 2 section 3.2.4. [incident response
2015-OE-0001	11/19/2015	13	Develop policy to detect and remove unauthorized (rogue) connections and implement measures including ongoing discovery scanning. [remote access
2015-OE-0001	11/19/2015	15	Update policy and procedures to require that system owners conduct an annual system inventory validation. [contractor systems
2015-OE-0001	11/19/2015	16	Develop HUD enterprise measurement plans to measure the progress and effectiveness of automating, consolidating, and modernizing legacy IT systems
2015-OE-0001	11/19/2015	17	Finalize the agreement currently in development between OCIO and OA [Office of Administration], in order to document roles, responsibilities and procedures for protection of PII by HUD offices. [privacy

2015-OE-0001	11/19/2015	18	Develop a formal program plan, including objectives, tasks, and milestones. Estimate staffing needs based on plan/requirements; identify consequences and risks for failure to properly staff and execute the plan. [privacy]
2015-OE-0001	11/19/2015	20	Obtain federal agency best practice information and conduct a Gap Analysis to identify requirements and deficiencies. [privacy]
2015-OE-0002	9/30/2015	1	Develop a coordinated mission-critical system development life cycle replacement program for mission-critical systems
2015-OE-0002	9/30/2015	3	Finalize, apply, and strategically communicate all standard IT policy across OCIO and the program offices to ensure that there is a common understanding of the modernization, EA, and CPIC policies
2015-OE-0002	9/30/2015	4	Approve at appropriate levels, Implement, and disseminate policy & processes as intended
2015-OE-0002	9/30/2015	8	Validate the accuracy of IT investment lists by segment and the associated projects and ensure alignment with EA strategy
2015-OE-0002	9/30/2015	9	Define and assess measurements in a yearly EA value measurement report in accordance with OMB EA framework guidance
2015-OE-0002	9/30/2015	10	Fully develop, approve at appropriate levels, and disseminate current CPIC process policies and procedures
2015-OE-0002	9/30/2015	11	Ensure that the Executive Investment Board meets in accordance with IT governance policy (related to recommendation from GAO-15-56)
2016-OE-0002	7/6/2017	3	We recommend that HUD enforce the requirement for all HUD web applications and services to be approved and authorized by OCIO.
2016-OE-0002	7/6/2017	4	We recommend that HUD evaluate the vulnerability findings identified by OIG and implement the associated technical recommendations.
2016-OE-0002	7/6/2017	8	We recommend that HUD establish and enforce a minimum frequency for password resets for all applications.
2016-OE-0002	7/6/2017	9	We recommend that HUD ensure that OCIO reviews and approves all IT contracts and service agreements dealing with creation or support of web applications or services.
2016-OE-0004S	3/29/2017	1	We recommend that the Director for the Office of Field Management ensure that the CDBG-DR risk analysis worksheet includes risk factors that show the measurement of performance outputs to determine completed activities.
2016-OE-0004S	3/29/2017	2	We recommend that the Director for the Office of Field Management update the risk analysis guidance for CDBG-DR grants to include the assessment of the likelihood of risk occurrence to help inform management which critical risks to address during monitoring.
2016-OE-0006	11/25/2016	2	The CIO should develop and implement an IT enterprisewide risk management program that aligns with the Agency's evolving enterprise risk management program
2016-OE-0006	11/25/2016	9	OCIO and OCHCO should identify the skills of personnel with significant security and privacy roles and responsibilities, provide training tailored to those roles and responsibilities, and implement human capital strategies to close identified skills gaps. This recommendation replaces FY 2015 recommendation number 9
2016-OE-0006	11/25/2016	11	OITS and OCHCO should provide the same HUD IT security awareness course to all HUD employees (government or contractor)

2017-OE-0007	10/31/2017	1	OCIO's risk office should review its role to add oversight efforts on information security risk. [This aligns with FY 2016 FISMA recommendation 2.] [Risk Management]
2017-OE-0007	10/31/2017	3	HUD should use qualitative and quantitative performance metrics to report on and monitor information security performance of its contractor-operated systems and services. [Contractor Systems]
2017-OE-0007	10/31/2017	5	OCIO should ensure that all HUD third-party or cloud applications route through the HUD TIC access points. [Configuration Management]
2017-OE-0007	10/31/2017	7	OCIO should require all POE used to connect to HUD's network to be properly configured, have written authorization, and be properly documented before connecting to HUD's network. [Identity and Access Management]
2017-OE-0007	10/31/2017	8	OCIO should require users who use POE to connect remotely to sign an agreement to forfeit the POE for analysis when security incidents occur. [Identity and Access Management]
2017-OE-0007	10/31/2017	12	OCIO should conduct an assessment of ISCM policies to determine where objectives have or have not been met and to prioritize future tasks. [Continuous Monitoring]
2017-OE-0007	10/31/2017	14	OCIO should implement an ongoing and continual control assessment and system authorization process. [Continuous Monitoring]
2017-OE-0007	10/31/2017	15	OCIO should ensure that the HUD CIRT has full capability to access all data and systems and leverage all tools necessary to conduct incident handling, response, containment, eradication, and monitoring activities. [Incident Response]
2017-OE-0007	10/31/2017	17	OCIO should establish measurement metrics and assign responsibility to track the effectiveness of the agency contingency planning activities. [Contingency Planning]
2017-OE-0007	10/31/2017	18	OCIO and the ERM Office should integrate contingency planning activities with agency enterprise risk management program activities. [Contingency Planning]
2017-OE-0007	10/31/2017	19	OCIO should integrate contingency plan testing activities with incident response testing activities at the enterprise level. [Contingency Planning]
2018-OE-0001	9/13/2018	3	Document the roles and specific responsibilities of all positions assigned privacy responsibilities. B. Communicate these responsibilities on a recurring basis, at least annually, to individuals holding these positions.
2018-OE-0001	9/13/2018	4	Implement thorough human capital processes to ensure execution of the HUD privacy program and all its requirements
2018-OE-0001	9/13/2018	6	Ensure the privacy program is integrated with the enterprise risk program and that privacy risks are incorporated into the agency risk management process
2018-OE-0001	9/13/2018	9	Develop a dedicated budget to address Privacy Office training needs and initiatives
2018-OE-0001	9/13/2018	10	Update all privacy guidance to reflect current Federal requirements and processes.
2018-OE-0001	9/13/2018	14	Ensure role-based privacy training is provided to all personnel with privacy responsibilities
2018-OE-0001	9/13/2018	15	Ensure privacy awareness training is provided to all contractor and third party personnel
2018-OE-0001	9/13/2018	19	Determine if general support system privacy threshold assessments or privacy impact assessments should be completed; if not, document the rationale

2018-OE-0001	9/13/2018	20	Develop the technical capability to identify, inventory, and monitor the existence of PII within the HUD environment
2018-OE-0001	9/13/2018	21	Develop and implement a process to inventory all agency PII holdings not less than annually. [Dependent upon completion of Recommendation 20
2018-OE-0001	9/13/2018	22	Renew the PII minimization effort, to include a prioritization by the SAOP of specific minimization initiatives
2018-OE-0001	9/13/2018	23	Require all system owners to review the records retention practices for each information system and take any corrective actions necessary to ensure adherence to the applicable records retention schedule
2018-OE-0001	9/13/2018	24	A. Issue a clean desk policy prohibiting unattended and unsecured sensitive data in workplaces. B. Implement procedures to enforce the clean desk policy.
2018-OE-0002	6/12/2018	2	We recommend that the Assistant Secretary for Administration periodically provide training on the occupant emergency plan once it is updated
2018-OE-0003	10/31/2018	1	HUD OCIO should develop a policy that: a. Defines how it will inventory web applications b. Includes how stakeholders must report the use of public-facing web applications (derived from OIG FISMA metric 1)
2018-OE-0003	10/31/2018	5	HUD OCIO should update software configuration management procedures to d. Require program offices to maintain cost estimates of tools and staffing to implement configuration management activities (derived from OIG FISMA metric 14). e. Include ongoing identification and mitigation of security risks with configuration changes (derived from OIG FISMA metric 15). f. Require lessons learned input for configuration changes (derived from OIG FISMA metric 15)
2018-OE-0003	10/31/2018	7	UD OCIO should develop a policy requiring programing offices to document their common secure configurations (derived from OIG FISMA metric 18)
2018-OE-0003	10/31/2018	8	HUD OCIO should implement and formally document a regularlyscheduled credentialed (authenticated) vulnerability scan program of all network components and applications, including web applications, in accordance with HUD risk management decisions. This recommendation replaces FY 2015 recommendation number 2 and updates FY 2016 recommendation number 4 (derived from OIG FISMA metric 18)

2018-OE-0003	10/31/2018	10	<p>HUD OCIO should update the HUD IT Security Policy Handbook 2400.25, Revision 4, to</p> <p>a. Assign responsibility for ensuring ICAM policies and procedures are annually reviewed and the completion date of the review is reflected within the document history (derived from HUD IT Security Policy Handbook 2400.25, sections 4.1.1, 5.1.1, 5.2.1, and OIG FISMA metric 23).</p> <p>b. Reflect current ICAM business processes (derived from HUD IT Security Policy Handbook 2400.25, section 2.22, and OIG FISMA metric 23).</p> <p>c. Account for how Rules of Behavior should be maintained for HUD web application users, such as Federal Housing Administration Connection business partners, that do not have direct access to HUD's network (derived from HUD IT Security Policy Handbook 2400.25, section 3.2.3, and OIG FISMA metric 27).</p> <p>d. Instruct program offices how to record reviews of user accounts, an inventory of privileged users, and lists of users by type and role (derived from HUD IT Security Policy Handbook 2400.25, section 5.2.2, and OIG FISMA metric 30).</p> <p>e. Require program offices to document non-public web applications as a type of remote access connection (derived from HUD IT Security Policy Handbook 2400.25, section 5.2.13, and OIG FISMA metric 31)</p>
2018-OE-0003	10/31/2018	11	<p>HUD OCIO should communicate to system owners the need to define and document an ICAM role within system application documentation (derived from OIG FISMA metric 23)</p>
2018-OE-0003	10/31/2018	12	<p>HUD OCIO should develop a FICAM segment architecture describing the performance, business, data, service, and technical architectures supporting HUD's ICAM processes (derived from OIG FISMA metric 24)</p>
2018-OE-0003	10/31/2018	14	<p>HUD OCIO should publish the system use notification statements that should be used on internal and external systems and web applications (derived from OIG FISMA metric 27)</p>
2018-OE-0003	10/31/2018	16	<p>HUD OCIO should require program offices to implement monitoring for web applications for potential anomalous data exfiltration (derived from OIG FISMA metric 35)</p>
2018-OE-0003	10/31/2018	17	<p>HUD OCIO should tailor the Security Awareness Training to be aligned to HUD's mission, information types, and its operating environment (derived from OIG FISMA metric 41)</p>
2018-OE-0003	10/31/2018	18	<p>HUD OCIO should conduct and document annual ISCM strategy reviews and lessons learned to make improvements to the ISCM Strategy (derived from OIG FISMA metrics 46 and 47)</p>
2018-OE-0003	10/31/2018	19	<p>HUD OCIO should integrate clear visibility into assets, awareness of threat information, and mission and business impacts into the ISCM strategy of all HUD web application systems (derived from OIG FISMA metric 46)</p>
2018-OE-0003	10/31/2018	20	<p>HUD OCIO should create a capability to develop and analyze qualitative and quantitative performance measures to report on the effectiveness of the ISCM program (derived from OIG FISMA metric 48)</p>
2018-OE-0003	10/31/2018	22	<p>HUD OCIO should implement a process to automate monitoring the authorization of all hardware assets on HUD's CDM dashboard (derived from OIG FISMA metrics 17 and 49)</p>

2018-OE-0003	10/31/2018	23	<p>HUD OCIO should update incident response operating procedures to</p> <p>a. Require the incident response plan to be reviewed annually and the document history updated appropriately (derived from OIG FISMA metric 52).</p> <p>b. Assign responsibility of analyzing current data loss prevention metrics and report them to appropriate personnel (derived from OIG FISMA metrics 54 and 58).</p> <p>c. Establish a metric that will measure the time for sharing incident information to incident response stakeholders (derived from OIG FISMA metric 56)</p>
2018-OE-0003	10/31/2018	25	<p>HUD OCIO should develop a process to automate the integration of logs from all end user workstations and all HUD servers into a single security incident and event management solution (derived from OIG FISMA metric 54)</p>
2018-OE-0003	10/31/2018	26	<p>HUD OCIO should develop a process, such as a dashboard, to continually measure and report the impact of incidents (derived from OIG FISMA metric 55)</p>
2018-OE-0003	10/31/2018	27	<p>HUD OCIO should implement a file integrity solution for workstations and servers (derived from OIG FISMA metric 58)</p>
2018-OE-0003	10/31/2018	28	<p>HUD should coordinate system contingency plans with the enterprise COOP and BCP (derived from OIG FISMA metric 64)</p>
2018-OE-0003	10/31/2018	29	<p>HUD OCIO should assign responsibility for consolidating system business impact assessment analyses to improve contingency plan implementation (derived from OIG FISMA metric 61)</p>
2018-OE-0003	10/31/2018	30	<p>HUD should test ISCP's during the HUD COOP testing (derived from OIG FISMA metrics 63 and 64)</p>
2018-OE-0004	8/13/2018	3	<p>We recommend that the Deputy Secretary direct PIH and OCIO to ensure that the Section 184 program transitions away from dependency on CHUMS.</p>
2018-OE-0004	8/13/2018	4	<p>We recommend that OCIO continue to develop required ONAP-LOS capabilities using cloud environments as appropriate</p>
2018-OE-0004	8/13/2018	5	<p>We recommend ONAP 5. Coordinate and participate in resolving all open recommendations from evaluation report IT System Management and Oversight of the Section 184 Program (2018-OE-0004)</p>
2019-OE-0001	2/4/2020	1	<p>refer troubled PHAs directly to the Assistant Secretary for Public and Indian Housing when they have not met the 1- or 2-year recovery requirements.</p>
2019-OE-0001	2/4/2020	2	<p>We recommend that the Director of the Office of Field Operations ensure that referrals to the Assistant Secretary for Public and Indian Housing recommend only recovery options allowed by the law and regulations.</p>
2019-OE-0001	2/4/2020	3	<p>We recommend that the Director of the Office of Field Operations update training to include the actions that PIH must take when a troubled PHA does not meet the 1- or 2-year recovery requirements.</p>
2019-OE-0001	2/4/2020	4	<p>We recommend that the Director of the Office of Field Operations provide training on remedies for long-term troubled PHAs to All PIH staff members who routinely interact with troubled PHAs.</p>
2019-OE-0002	6/24/2020	1	<p>The OIG has determined that the contents of this recommendation would not be appropriate for public disclosure and has therefore limited its distribution to selected officials.</p>

2019-OE-0002	6/24/2020	17	The OIG has determined that the contents of this recommendation would not be appropriate for public disclosure and has therefore limited its distribution to selected officials.
2019-OE-0002	6/24/2020	18	The OIG has determined that the contents of this recommendation would not be appropriate for public disclosure and has therefore limited its distribution to selected officials.
2019-OE-0002	6/24/2020	19	The OIG has determined that the contents of this recommendation would not be appropriate for public disclosure and has therefore limited its distribution to selected officials.
2019-OE-0002	6/24/2020	20	The OIG has determined that the contents of this recommendation would not be appropriate for public disclosure and has therefore limited its distribution to selected officials.
2019-OE-0002	6/24/2020	21	The OIG has determined that the contents of this recommendation would not be appropriate for public disclosure and has therefore limited its distribution to selected officials.
2019-OE-0002	6/24/2020	22	The OIG has determined that the contents of this recommendation would not be appropriate for public disclosure and has therefore limited its distribution to selected officials.
2019-OE-0002	6/24/2020	23	The OIG has determined that the contents of this recommendation would not be appropriate for public disclosure and has therefore limited its distribution to selected officials.
2019-OE-0002	6/24/2020	24	The OIG has determined that the contents of this recommendation would not be appropriate for public disclosure and has therefore limited its distribution to selected officials.
2019-OE-0002	6/24/2020	25	The OIG has determined that the contents of this recommendation would not be appropriate for public disclosure and has therefore limited its distribution to selected officials.
2019-OE-0002	6/24/2020	26	The OIG has determined that the contents of this recommendation would not be appropriate for public disclosure and has therefore limited its distribution to selected officials.
2019-OE-0002a	6/25/2020	1	Designate a Senior Agency Official for Records Management at the Assistant Secretary level or its equivalent.
2019-OE-0002a	6/25/2020	2	Update and issue agency formal records policy, including detailed procedures and requirements for completing and maintaining program office and agencywide inventories of systems, records, and PII.
2019-OE-0002a	6/25/2020	3	Update and obtain final NARA approval of all HUD records retention schedules, including the Capstone email schedule, to comply with Federal requirements, including OMB M-19-21.
2019-OE-0002a	6/25/2020	4	Develop and approve an enterprise strategy to meet all M-19-21 electronic transition requirements.
2019-OE-0002a	6/25/2020	5	Issue a formal policy and requirements for managing CUI.
2019-OE-0002a	6/25/2020	6	Establish and disseminate a policy on safeguarding or prohibiting the transportation of PII records out of the office for telework purposes.
2019-OE-0002a	6/25/2020	7	Complete the development of performance measures and establish a formal records evaluation process to measure the effectiveness and progress of the records management program.
2019-OE-0002a	6/25/2020	8	Standardize processes and duties for all RMLOs.

2019-OE-0002a	6/25/2020	9	Conduct a staffing resource assessment for the HUD records program and identify any skills gaps or resource needs.
---------------	-----------	---	--