U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
WASHINGTON, D.C. 20410-3000

MEMORANDUM FOR: Distribution

DATE ISSUED: May 7, 2020

FROM: David C. Chow, Chief Information Officer, Q

John Bravacos, Senior Agency Official for Privacy, D

THORUGH: Hun S. Kim, Chief Information Security Officer, QS

Ladonne White, Chief Privacy Officer, AHFC

SUBJECT: Privacy Office Memorandum 02-00, Authorization to Operate (ATO) and Privacy Impact Assessment (PIA) Requirements to Launch Information System into Production

The Office of the Chief Information Officer (OCIO) is committed to complying with Federal regulations in order to secure and protect critical HUD assets, including Department information systems and data. **OCIO would like to remind all Program Offices of the requirements for all HUD applications and systems[1] to: (1) complete the Security Assessment and Authorization process (2) receive an Authorization to Operate (ATO) and (3) complete a Privacy Impact Assessment (PIA) prior to release into production.**

ATO Requirements for Program Offices

As outlined in the Federal Information Security Modernization Act of 2014 (FISMA 2014), the NIST Special Publication 800-37, Revision 2: *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* and HUD's IT Security Policy Handbook, **all systems and applications must undergo Security Assessment and Authorization activities prior to release into production**. This includes systems and applications that are currently designated as Minor Applications, Cloud Services, Websites, and Contractor Owned and Operated systems and applications. Effective immediately all Security Assessments are to be conducted by the Office of Information Technology Security (OITS), with the exception of HUD Office of the Inspector General (HUD OIG) and Ginnie Mae (GNMA). Additionally, Program Offices are to cease conducting security self-assessments.

Operating a system without an ATO creates significant security risks that may compromise the confidentiality, integrity, and availability of HUD's assets and data. Without the appropriate assessment of information systems' security posture, the organization will not have visibility into its security weaknesses, ultimately making HUD susceptible to a data breach or privacy incident with catastrophic long-term impacts. If the risk to the organization is too high, it

[1] All systems are defined as Minor Applications, Major Applications, General Support Systems, Cloud Services, Websites, Contractor Owned or Operated Systems and Applications.

is possible that OCIO may recommend disabling the use of the unauthorized systems per Executive Order 13833: *Enhancing the Effectiveness of Agency Chief Information Officers*.

In order to launch a system into production, Program Offices must complete the following actions:

1. For systems that are in the planning, development, or testing phase, System Owners shall collaborate with the Office of Information Technology Security (OITS) to develop a project plan and schedule for completing the Security Assessment and Authorization process within 90 days of receipt of this memo. All Security Assessment and Authorization process should be completed 60 days prior to planned deployment.
2. For systems and applications that are currently in production without an ATO, System Owners shall prepare and submit a Risk Based Decision (RBD) Memorandum to the CISO, within 30 days of receipt of this memo, requesting authorization to continue to operate until the Security Assessment and Authorization process is completed. The RBD at a minimum should include the following:
    a. Overview of the system/application describing the mission/purpose of the system/application.
    b. Rationale as to why the RBD is required.
    c. Current security controls in place.
    d. Identify compensatory controls that will be implemented until the Security Assessment and Authorization process is completed and an ATO is issued.
    e. The RBD shall not extend beyond120 days.
3. Refer to the ATO Prep List attachment accompanying this memo to for requirements to complete the Security Assessment and Authorization process.

PIA Requirements for Program Offices

In addition to ATO requirements, **all Program Offices are required to complete a PIA for each HUD information system, General Support Systems, or electronic collection** that collects, maintains, uses, and/or disseminates PII about US citizens, Federal employees, and HUD contractors. Please note, the Privacy Office and OCIO recently announced the release of an **updated PIA form**. The new, user-friendly PIA form and its accompanying Reference Guide are available on the HUD@Work Privacy Office page, as well as on the public-facing Privacy site. The Privacy Office is available to answer any questions at privacy@HUD.gov.

OCIO is eager to collaborate with Program Offices on these activities to protect and secure HUD's valuable assets while avoiding a delay in production of any HUD information system. Thank you for your continued attention to HUD's data integrity and security. Please contact Hun Kim, Hun.S.Kim@hud.gov, the Chief Information Security Officer (CISO), and LaDonne L. White, Ladonne.L.White@hud.gov, the Chief Privacy Officer (CPO) for follow-on actions and/or questions.

FOR DISTRIBUTION:

- All Authorizing Officials (AOs)

- All Information System Security Officers (ISSOs)
- All System Owners