U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

Office of the Chief Information Officer

Special Attention of: **Transmittal for Handbook No: 2400.25 REV-2 Chg-2**

Issued: 4/14/11

1. This Transmits: HUD Handbook 2400.25 REV-2 Chg-2 , Information Technology Security Policy

2. Summary:

In response to FHA FY 2010 Financial Statement Audit - Management Letter Findings, Rec. 3A, the Office of IT Security is submitting through the departmental clearance process a change to the HUD IT Security Policy Handbook 2400.25 Rev-2. Below are the proposed changes that will be reflected in Handbook 2400.25 Rev-2 Chg-2

Rev-2 Chg-2 - Section 3.1.5 Vulnerability Scanning

RA-5:

a. OCIO ensures HUD's infrastructure, including the LAN, WAN, Internet, Intranet, Enterprise mainframe(s), etc., is regularly scanned. Vulnerability scans of subnets are conducted weekly such that the entire network is scanned over a 12 month period. OCIO shall ensure monthly scans for patch status.
b. Program Offices/System Owners shall ensure applications under their control are scanned for vulnerabilities, e.g. code reviews including static, dynamic & web based code, during system development, prior to new releases, or when there are major changes to the application.
c. OCIO uses the National Vulnerability Database (NVD) [http://nvd.nist.gov/ (url pulled 6-1-2010)] repository as their vulnerability checklist and stays current with NVD updates as well as vendor advisories and system vulnerability scanning information to ensure that significant vulnerabilities impacting HUD information systems are identified and reported.

OCIO shall ensure that vulnerabilities with a CVE score of 7.5 or higher are remediated within ninety days or a remediation task is created in the System's POA&M.

Rev 2 Chg-2 Section 4.3.2 Contingency Plan

CP-2:

a. Program Offices/System Owners shall develop contingency plans, including a Business Impact Analysis, for information systems under their purview in accordance with HUD *Contingency Plan Guidance* and NIST SP 800-34: *Contingency Planning Guide for Federal Information Systems.*

b. Program Offices/System Owners shall, as part of their Business Impact Analyses, complete a HUD Mission Critical Questionnaire which becomes part of the system security planning package.

c. For moderate- or high-impact systems, Program Offices/System Owners shall coordinate with the Program Office(s) responsible for Critical Infrastructure Protection (CIP) and Continuity of Operations (COOP).

d. For high-impact systems, Program Offices/System Owners, in conjunction with the Deputy CIO for IT Operations, shall conduct capacity planning so that the necessary capacity for information processing, telecommunications, and environmental support exists during crisis situations.

e. Program Offices/System Owners shall develop a list of key individuals with contingency roles and responsibilities

f. Program Offices/System Owners shall make the contingency plans, and any updates, available to these key individuals.

g. OCIO shall establish and maintain a HUD-CIRT to prevent, detect, track, and respond to information security incidents and alerts in accordance with NIST SP 800-61, *Computer Security Incident Handling Guide*. (see IR-4)

h. Program Offices/System Owners shall review contingency plans once a year generally in conjunction with the annual contingency plan test, update the plans as necessary and communicate any changes to the Program Office(s) responsible for COOP and CIP.

Filing Instructions:

Remove:	Insert:
Section 3.1.5 HUD Handbook 2400.25, Rev-2, p.18, dated 11/30/09	HUD Handbook 2400.25, Rev-2 Chg-2. ,dated 8/24/10
Section 4.3.2 HUD Handbook 2400.25, Rev-2 p.52 11/30/09	HUD Handbook 2400.25, Rev-2 Chg-2. ,dated 10/26/10

Distribution: W-3-1