

NATIONAL SUPPLEMENT
Between
U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
and
AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES
NATIONAL COUNCIL OF HUD LOCALS 222

Subject: HUD Handbook 2400.24, REV-2, Information Security Program

1. **Scope.** The scope of this agreement relates to the impact and implementation of Management's proposed Handbook 2400.24, REV-2, Information Security Program.
2. **Purpose.** The purpose of this supplement to the Information Security Program Handbook is to balance the statutory and regulatory requirements that the Department adequately protect the security of the data and information of its systems, while ensuring that such information security requirements do not deny, as stated in Executive Order 10450, "individual employees fair, impartial, and equitable treatment at the hands of Government, or rights under the Constitution and laws of the United States or this order."
3. **Corrections to Background Investigation.** Employees will be given an opportunity to correct or add to the records of an ongoing background investigation.
4. **Sensitivity Levels.** The parties agree that the sensitivity of positions will be determined in relation to the sensitivity level(s) of Departmental systems accessed by employees, and that such sensitivity relates to system-by-system designation as to its data sensitivity and mission criticality of the Department.. Any determination that an employee must undergo a security screening will be based strictly on sensitivity level(s) of Departmental systems accessed by the employee.

The Union will be given notice of the sensitivity level of all sensitive systems, which will be updated annually and provided by Management.

5. **Orientation and Training.** As a part of new employee orientation, all entering HUD employees will receive, as a part of their Orientation Process, materials describing their responsibilities relative to their potential access and use of sensitive and critical data or systems. The Union will receive an advance copy of orientation materials intended for the new employees. Employees will be required to acknowledge receipt of such materials.

Training on information security awareness and practices will be provided to employees annually. The Union will receive copies of any materials distributed during this training.

6. **Debriefing.** Supervisors shall debrief all employees terminating assignments with sensitive systems. Such debriefings will constitute such discussions as employee reminders regarding non-disclosure of sensitive data to which employees may have been exposed. The contents of these debriefings will contain the standard elements identified in Section 5-14 of the Information Security Program Handbook. Management will identify to the employees those permissible persons to whom subsequent disclosures may be made, if any, the nature of the sensitive material which should not be disclosed. Employees will be briefed on their continuing responsibilities and will be asked to sign an acknowledgment of receipt of such debriefing.

7. **Access Removal.** Management should provide notice to the Union and employee at the time it removes an employee's access to sensitive materials.

8. **Sensitive Position Designations.** Management determinations regarding sensitive position designations will be made in accordance with applicable law and regulation. A determination as to position sensitivity regarding other programs will be made independent of the provisions of the HUD Handbook on Information Security, based on criteria of those programs.

9. **Grievances.** The negotiated grievance procedure will be available with respect to any personnel actions resulting from findings made in connection with the Information Security Program Handbook. This provision in no way diminishes the availability of employees' rights to grieve in accordance with the Master Agreement between the parties.

10. **Penalties.** Whenever "penalties" are discussed in the Information Security Program Handbook, the meaning shall be in accord with the concept of "progressive discipline" as stated in Section 20.02(3) of the HUD/AFGE Agreement.

11. **Positions Identified for Background Investigations.** Management will make every effort to keep to a minimum those positions requiring security background investigations, consistent with prudent deployment of staff and program mission accomplishment. However, when positions have been designated as requiring security background investigations, the incumbents must meet security requirements. Employees who choose not to undergo Background Investigation which would be required because of a position's information security sensitivity may be reassigned to other available positions at management's option.

12. **Password Disclosure.** Non-negligent, inadvertent disclosure of one's password shall not necessitate disciplinary action.

13. **Security Standards.** HUD's Information Security Program Handbook standards are promulgated in accordance with the standards established by the Secretary of Commerce pursuant to the Computer Security Act of 1987, and other relevant laws, rules and regulations

14. **Uniform Criteria.** The criteria used to assess the sensitivity and criticality of HUD information systems, and the positions within those systems, will be uniformly applied on a Departmentwide basis.

15. **Privacy Act Training.** Information Security Program Handbook training will include appropriate treatment of the requirements of the Privacy Act.

16. **Union Receipt of Background Investigation Lists.** As the information identifying positions requiring Background Investigations becomes available, the Union will receive lists of those affected positions.

17. **Lack of Opportunity for Training.** Management will give appropriate consideration to an employee's lack of opportunity to attend Information Security Program training during any determination of the consequences of the employee's violation of security requirements.

18. **Allegation of Security Breach.** In determining whether disciplinary action is appropriate with respect to a security breach, management will weigh all of the relevant facts, including whether the breach was a mere allegation.

19. **Repeat Background Investigations.** Employees who have undergone the appropriate Background Investigation and can demonstrate its currency, will not be required to undergo another one unless their current job requires a higher level of investigation or the period of the current investigation expires.

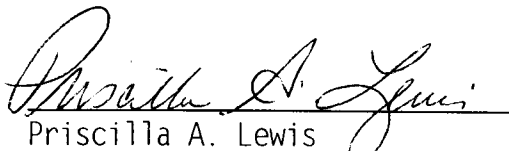
20. **Vacancy Announcements.** Management will place the following statement on all vacancy announcements:

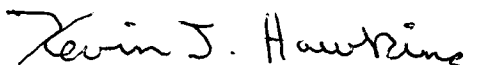
Positions in the Federal service are subject to investigation. You may be asked to complete the necessary forms (SF 85, SF 85P or SF 86) to meet that requirement. Applicants having questions regarding a specific form to be used should contact the Personnel representative.

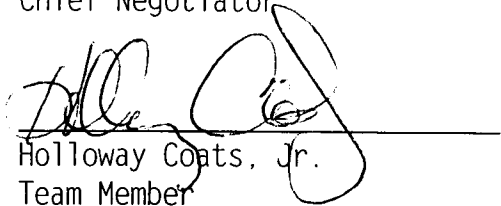
21. **PD's and EPPES.** Where appropriate, management will review and amend position descriptions and/or performance standards to reflect any changed or additional duties relating to information security.
22. **Access to Systems.** The Department will ensure that systems security controls will be consistently applied so as to enable adequacy of employees' security access to systems required to accomplish position functions.
23. **Information Security Reviews.** When possible, employees and the Union will be notified of management's intent to perform planned reviews of information security in a specific work environment.
24. **Information Security Implementation.** With regard to implementing information security systems responsibilities, management will make every effort to minimize the effect on employees.
25. **Reassignment.** Employees who choose not to undergo Background Investigations which would be required because of a position's information security sensitivity may be reassigned to other available positions at management's option. Employees choosing to leave such positions may do so without prejudice.
26. **Privacy Rights.** Management agrees that employees' personal computers and related equipment are subject to employees' rights to privacy in accordance with Section 4.09(7)(a) of the HUD/AFGE Agreement.
27. **Background Investigations.** Management agrees that employees have a right to consult with the Union at the time that a Background Investigation form is provided to the employee. Management further agrees that completed background investigations forms will not be accessible to the employees supervisors. They will be submitted directly to the Personnel Security Staff. After the investigations have been completed, the employees' supervisor will only be advised of adverse information on a need to know basis.
28. **Investigatory Interviews.** Management agrees that in conjunction with meetings regarding adverse information resulting from a background investigation, employees have the right to representation in accordance with Section 4.08 of the HUD/AFGE Agreement.
29. **Supplement Reference.** The following statement will be added to the Transmittal sheet for Handbook 2400.24, REV-2: "Bargaining unit employees should also refer to any negotiated labor/management agreements regarding the Information Security Program."

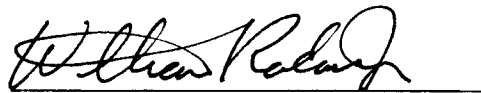
Management

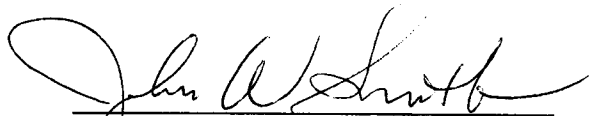
AFGE



Priscilla A. Lewis
Chief Negotiator



Kevin J. Hawkins
Chief Negotiator


Holloway Coats, Jr.
Team Member



William L. Radau
Team Member


John W. Smith
Team Member


Ann Taylor
Team Member


Sherry K. Norton
Team Member

Approved: 
Director, Office of
Human Resources

Approved: 
Mortimer F. Coward
President, AFGE
National Council
of HUD Locals 222

Date: 11/10/99

Date: 11/3/99