

ATTACHMENT 11- EIV SECURITY CHECKLIST

EIV SECURITY CHECKLIST

SECURITY ASSESSMENT		
<i>Reviewers should review the Owner's/Agent's (O/A's) (1) security policies and procedures; (2) security and system access files; and (3) any other documents that will provide answers to the questions below. Reviewers may also want to conduct an interview with the O/A and/or other designated staff persons that have knowledge of the O/A's security procedures and policies and are able to respond to the questions below.</i>		
Questions – Place an “X” in the applicable box.	Yes	No
1. Does the O/A have a designated Security Office or equivalent?		
2. Does the O/A have a Security Policies and Procedures document?		
3. Does the O/A enforce security procedures?		
4. Does the O/A keep records and monitor security issues?		
5. Does the O/A conduct and document Security Awareness Training for EIV system users?		
6. Does the O/A maintain a record of all EIV system users and their assigned roles?		
7. Does the O/A ensure that each user has and uses his/her own user ID and password?		
8. Does the O/A maintain copies of signed and access authorization and rules of behavior/user agreement forms for all EIV system users and coordinators?		
9. Does the O/A maintain copies of the completed and signed Security Awareness Training Questionnaires for all EIV system users and coordinators?		
10. Does the O/A conduct a quarterly review of all EIV User Ids to determine if users still have a valid need to access UIV data? (EIV quarterly User Certification process)		
11. Does the O/A maintain a key control log to track the inventory of keys available for secure rooms, buildings or file cabinets?		
12. Does the O/A maintain a log of all destroyed EIV system documents or have a record retention policy?		
13. Does the O/A have valid (dated within the last 15 months) HUD-9887s in the reviewed tenant files?		
14. Does the O/A document the occurrence of all improper disclosures of EIV system information in writing or have a procedure to document improper disclosures?		
15. Does the O/A report any occurrence of unauthorized access or known security breaches to the designated HUD staff person(s) or have a procedure to report an occurrence of unauthorized access or known security breaches to the designated O/A/HUD staff persons(s)?		
16. What security methods does the O/A use to provide physical security of EIV system data? <i>Check all that apply:</i> () Restricted areas () Locked rooms () Locked file cabinets () None		

<input type="checkbox"/> Other (please specify)		
17. How does the O/A dispose of EIV information once the data retention period has expired? Check all that apply. <input type="checkbox"/> Burn <input type="checkbox"/> Shred <input type="checkbox"/> Erase <input type="checkbox"/> Other (please specify) <input type="checkbox"/> None		