



Issue Date July 28, 2011

Audit Report Number 2011-DP-0008

TO: Yolanda Chávez, Deputy Assistant Secretary for Grant Programs, DG
Jerry Williams, Chief Information Officer, Q

//s//

FROM: Hanh Do, Director, Information Systems Audits Division, GAA

SUBJECT: The Disaster Recovery Grant Reporting System that Maintained Recovery Act Information Had Application Security Control Deficiencies

HIGHLIGHTS

What We Audited and Why

We audited the Disaster Recovery Grants Reporting (DRGR) system to determine whether adequate controls were in place to safeguard and accurately track and report \$1.93 billion in American Recovery and Reinvestment Act of 2009 (ARRA) funds allocated to the Office of Community Planning and Development's (CPD) Neighborhood Stabilization Program 2. Specifically, we reviewed the implementation of application controls over business processes, interfaces, and data management systems. The assignment was initiated to address ARRA's requirement for reporting accurate data. The results will be used to support our annual review of the U.S. Department of Housing and Urban Development's (HUD) consolidated financial statements.

What We Found

CPD had improved the DRGR system within the last year. Specifically, it had

1. Established policies and procedures for user access requests and completion of user rules of behavior before granting the user access to the system,
2. Updated configuration management plans,
3. Created an application system and user manuals, and
4. Ensured that contractors tested both drawdown controls and computer processes in accordance with regulations.

CPD's improvements to the DRGR system were beneficial to the overall assurance that the system's data were properly maintained, safeguarded, and in compliance with Federal regulations. In order for HUD to address ARRA requirements for accurate data requirements, improvements should be made to the DRGR system. [REDACTED]

Management attention is also needed to address application controls over business processes. For example, security management is lacking in the areas of security documentation, vulnerability scans, and contingency plan testing. Also, to ensure that DRGR system data are secure, application security management needs to be effectively implemented.

What We Recommend

[REDACTED] the DRGR system owner needs to coordinate with the Office of the Chief Information Officer (OCIO) to ensure that vulnerability scans are completed, security documentation is updated, and the contingency plan is adequately tested.

We also recommend that OCIO ensure that the DRGR system is included in the annual disaster recovery test as it is a mission-critical application.

For each recommendation without a management decision, please respond and provide status reports in accordance with HUD Handbook 2000.06, REV-3. Please furnish us copies of any correspondence or directives issued because of the audit.

Auditee's Response

We requested responses from OCIO and CPD to be received by July 8, 2011. We received written responses to the draft report from OCIO and CPD on July 8, 2011.

CPD requested changes to some of OIG's data elements included in the report and provided overall comments on the DRGR system [REDACTED]. OCIO suggested verbiage changes to recommendations for Finding #2. The complete text of OCIO's and CPD's response, along with our evaluation of that response, can be found in appendix A of this report.

TABLE OF CONTENTS

Background and Objective	5
Results of Audit	
Finding 1: [REDACTED]	7
Finding 2: Weaknesses Existed in the Application Security Management Program of the DRGR System	10
Scope and Methodology	14
Internal Controls	16
Follow-up on Prior Audits	17
Appendixes	
A. Auditee Comments and OIG's Evaluation	18

BACKGROUND AND OBJECTIVE

Operational since February 1999, the Disaster Recovery Grant Reporting (DRGR) system was developed by the U.S. Department of Housing and Urban Development's (HUD) Office of Community Planning and Development (CPD) for the Disaster Recovery Community Development Block Grant (CDBG) program and other special appropriations. Data from the system are used by HUD staff to review activities funded under these programs and for required quarterly reports to Congress. The system was developed for grantees to identify activities funded under their action plans and amendments, to include budgets and performance goals for those activities. To receive funding, these grantees must prepare a citizen participation plan, publish their proposed use of the funds, and submit an action plan to HUD. Once an action plan is submitted and approved, grantees can submit quarterly reports summarizing obligation, expenditures, drawdowns, and accomplishments for all of their activities.

On July 30, 2008, Public Law 110-289, the Housing and Economic Recovery Act of 2008 (HERA), was passed to provide housing reform. HERA designated HUD to distribute \$3.92 billion in Federal funds to States and local entities using the CDBG model. (The CDBG model is an entitlement program that distributes funds annually, by formula, to large communities and States as well as smaller communities and Indian reservations.) The HERA funds and distribution are known as the Neighborhood Stabilization Program (NSP) and are meant for the purchase and rehabilitation or development of foreclosed-upon or abandoned homes and residential properties. This program is now referred to as NSP1. Eligible uses include (1) establish financing mechanisms for purchase and redevelopment of foreclosed-upon homes and residential properties; (2) purchase and rehabilitate homes and residential properties that have been abandoned or foreclosed upon to sell, rent, or redevelop such homes and properties; (3) establish land banks¹ for homes that have been foreclosed upon; (4) demolish blighted structures; and (5) redevelop demolished or vacant properties.

The emergency nature of HERA and corresponding statutory timeframes did not give HUD sufficient time to develop a new system or modify an existing system to perfectly fit the program. Therefore, HUD decided to expand the use of the DRGR system application to include NSP1 in 2008. The DRGR system was selected for the program because no other application and reporting system was sufficiently flexible to deal with the alternative requirements. HUD made significant modifications to the system to allow for the reporting of specific activities under NSP1.

The American Recovery and Reinvestment Act of 2009 (ARRA) was passed on February 17, 2009, to provide competitive grant awards to States, units of general local government, and nonprofit organizations for economic recovery from the recession. It revised some of the program rules for NSP1 (HERA) and appropriated an additional \$2 billion for NSP to be competitively awarded. This program is now referred to as NSP2. The eligible uses noted for NSP1 were revised as follows: (1) "establish land banks for homes that have been foreclosed

¹ A land bank is a governmental or nongovernmental nonprofit entity established, at least in part, to assemble, temporarily manage, and dispose of vacant land for the purpose of stabilizing neighborhoods and encouraging reuse or redevelopment of urban property (Federal Register Notice 73 FR 58330).

upon” was modified by ARRA to read “establish and operate land banks for homes and residential properties that have been foreclosed upon,” and (2) ARRA added a provision to the use “redevelop demolished or vacant properties,” stating that funding used for section 2301(c)(3)(E) of HERA must be available only for the redevelopment of demolished or vacant properties as housing. In addition, ARRA repealed a section of HERA related to reinvestment of profits. ARRA also authorized the establishment of the NSP Technical Assistance (NSP-TA) program to improve the capacities of NSP grantees and the implementation of their programs. ARRA set aside \$50 million of the \$2 billion appropriation specifically for this purpose. NSP-TA grants were awarded to States, units of general local government, nonprofit organizations, and other organizations capable of providing technical assistance to the NSP grantees.

On July 21, 2010, Public Law 111-201, the Dodd-Frank Wall Street Reform and Consumer Protection Act, authorized \$1 billion in additional funds for NSP. This program is now referred to as NSP3. NSP3 provides formula grant awards to States and units of local government to undertake eligible activities as provided under HERA. In addition, up to 2 percent of the funds can be made available by HUD for technical assistance grants.

The objective of this review was to assess whether adequate system controls within the DRGR system were in place to safeguard, track, and report on ARRA NSP2 funding. Our review was focused on determining whether the security controls over business processes, interfaces, and data management systems, complied with generally accepted auditing principles and the U.S. Government Accountability Office’s Federal Information System Controls Audit Manual (FISCAM) elements.

RESULTS OF AUDIT

Finding 1:

[REDACTED] CPD was aware that [REDACTED] needed improvement; however, due to prioritizing tasks for the system with budgetary and staffing constraints, not all controls had been implemented. [REDACTED]



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

CPD did not follow industry guidance regarding [REDACTED] based on Federal Information Processing Standards Publication 200 (FIPS PUB 200), “Minimum Security Requirements for Federal Information and Information Systems.”

[REDACTED]

HUD Information Technology Security Policy, 2400.25, REV-2, CHG-1, also states that system owners are responsible for identifying events which require auditing [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

The system owner stated that the information technology (IT) budget had been used mainly to address new congressional requirements.

Conclusion

[REDACTED]

Recommendations

We recommend that the Office of Community Planning and Development

- 1A. Modify the DRGR system's [REDACTED]

Finding 2: Weaknesses Existed in the Application Security Management Program of the DRGR System

The DRGR program office's application security management program had weaknesses.

Specifically

[REDACTED]

(2) the DRGR system security documentation had not been updated to reflect current information about the system and its environment; and (3) although the DRGR system had been classified as a mission-critical system, it was not tested during the most recent annual disaster recovery test. These conditions occurred because DRGR program officials are responsible for communicating with the OCIO to ensure that security controls of their system are adequate and their system documentation is up to date, however they did not provide updated information to OCIO. As a result, the necessary security controls may not have been implemented. In addition, since the contingency plan had not been adequately tested the effectiveness of the plan or the system's readiness to deal with a potential disaster could not be determined.



In May 2009, OCIO completed a vulnerability scan analyzing several of the DRGR system's business processes.



FISCAM states that organizations need to "Implement effective application security management." Elements of an effective plan include

- "Periodically assess and validate application security risks
- Document and implement application security policies and procedures
- Monitor the effectiveness of the security program
- Effectively remediate information security weaknesses"

The condition described above occurred because the DRGR system owner did not monitor the effectiveness of the security management program



[REDACTED]

Without effective security management over the application, the DRGR system could not obtain reasonable assurance that the application was effectively secure.

The DRGR Program Office Did Not Have Up-to-Date Security Documentation for Its DRGR System

DRGR system security documentation (such as the security plan, risk assessment, and contingency plan) had not been updated for consistency and to address changes to the information system and its environment of operation. For example, the DRGR system's risk assessment (V6.5.3) showed the application categorized as a high-risk system and not a mission-critical system. However, the DRGR system's contingency plan (V6.5.3) categorized it as moderate risk and listed it as a mission-critical system. Also, the DRGR system's security plan (V6.5.3) stated that the system interfaced externally with the Line of Credit Control System (LOCCS) and the drawdowns created in the DRGR system were reconciled with LOCCS to ensure accuracy of financial balances. However, the DRGR system owner confirmed that the system did not automatically reconcile with LOCCS; rather, the owner used the reports generated by a third-party software reporting tool to reconcile the DRGR system drawdown data to LOCCS.

NIST SP 800-53, Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations," states that organizations should develop a security plan that "is consistent with the organization's enterprise architecture." It also states that organizations should "update the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments."

The above condition occurred because the DRGR system owner and its system security officers were not aware of the inconsistency in the system's security documentation. They explained that this inconsistency was a mistake and stated that they would review and update the documentation.

Without up-to-date system security documentation, risks associated with the DRGR system may not have been properly identified and addressed. Mission-critical and high-risk systems have different security requirements, and if documentation is not current, these requirements will not be enforced.

The DRGR Contingency Plan Had Not Been Adequately Tested

The DRGR system was categorized as a HUD mission-critical system, yet the application was not adequately tested as required by HUD Information Technology Security Policy, 2400.25, REV-2, CHG-1. Contingency plan testing for the DRGR system was conducted in November 2010, however it was not tested under conditions that simulate a disaster or test the restoration of operations. The security policy stated that “Program Offices/System Owners shall ensure that plans for moderate and high-impact systems are tested/exercised at least annually in compliance with the HUD contingency planning guidance and NIST SP 800-34.² Testing should be coordinated with elements responsible for COOP (continuity of operations plan), CIP (critical infrastructure protection) and incident response.” Also, NIST SP 800-34 specifically requires that “each information system component should be tested to confirm the accuracy of individual recovery procedures. This includes the “restoration of normal operations.”

The DRGR system had not been tested in the HUD disaster recovery test because its system classification had not been updated in the Cyber Security Assessment and Management system (CSAM)³ to reflect that it is a mission-critical system. OCIO bases the list of systems to be tested for annual disaster recovery on CSAM data, and because DRGR system data were not complete in CSAM, the DRGR system was not tested during the most recent disaster recovery test. OCIO was working with the IT contractor to address contract issues that would allow the DRGR system to be included in the next disaster recovery test.

By not conducting an adequate contingency plan test for the DRGR system the system owner could not determine the plan’s effectiveness and the organization’s readiness to execute the plan as intended in an emergency situation. Further, without validating one or more of the system components and the operability of the plan, the DRGR system owner would not be able to identify and address the deficiencies in the plan.

² NIST SP 800-34, “Contingency Planning Guide for Federal Information Systems”

³ The CSAM C&A (certification and accreditation) Web originated as the U.S. Department of Justice (DOJ) in-house application supporting the C&A process, plans of action and milestones management, and Federal Information Security Management Act (FISMA) reporting. HUD selected this DOJ shared service center as its FISMA reporting solution.

Conclusion

The DRGR system owner needs to improve its application security management program to fully address Federal guidelines. The DRGR system owner did not update security documentation and adequately test its contingency plan that allows appropriate risks to be addressed and proper security controls to be implemented.

[REDACTED]

Further, the contingency plan had not been adequately tested, to determine whether the plan could be successfully executed in an emergency situation.

Recommendations

We recommend that the Office of Community Planning and Development

2A. [REDACTED]

2B. Ensure that the DRGR system owner reviews and updates DRGR system security documentation to ensure that it is consistent and to address changes to the information system environment.

2C. Coordinate with HUD OCIO and contractors responsible for the disaster recovery test to perform the contingency plan test on the DRGR system that addresses restoration of normal operations.

We recommend that the Office of the Chief Information Officer

2D. Ensure that the DRGR system's contingency plan is tested in compliance with the HUD contingency planning guidance and NIST SP 800-34.

SCOPE AND METHODOLOGY

We conducted the audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective(s). We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

We performed the audit

- From February through June 2011.
- At HUD headquarters, Washington, DC.

To accomplish our objective, we

- Reviewed CPD's DRGR system documentation (such as functional requirements, data requirements, system security plan, and risk assessment) to gain an understanding of the system configuration, policies and procedures, and drawdown processes.
- Interviewed CPD management officials and users to understand the DRGR system processes, controls, and risks.
- Obtained computer-processed disbursement data from the HUD Central Accounting Processing System (HUDCAPS) for the period October 1, 2010, through March 31, 2011. We assessed the reporting controls for the DRGR system interface by (1) reviewing existing information about the data and the system that produced the data, (2) comparing data between HUD's financial reporting application system—HUDCAPS and the DRGR system, and (3) interviewing agency officials knowledgeable about the data. We determined that the data were sufficiently reliable for the purposes of this report.
- Reviewed and assessed the audit and accountability controls for the DRGR system.
- Assessed 77 business user activity features as described in the DRGR Operations Manual and Grantee User Manual. We selected 77 activities from a total of 103 business user activity features that were listed in the manuals. These 77 activities were objectively selected based on most common usability by the audit team [REDACTED]
- Reviewed DRGR system documentation to obtain a basic understanding of business functions [REDACTED]
- Determined whether the DRGR system grantees' reporting methodology complied with Office of Management and Budget guidance.
- Reviewed a subset of NSP2 grantees' data in the DRGR system and compared it to the data reported in FederalReporting.gov⁴ to determine whether the grantees' reporting data

⁴ FederalReporting.gov is the central nationwide data collection system for Federal Agencies and Recipients of Federal awards under Section 1512 of the Recovery Act. Recipients will access www.FederalReporting.gov in order to fulfill their reporting obligations. Federal Agency and Recipient users will be able to submit reports, view and comment on reports (Federal Agency and Prime Recipient users), and update or correct reports.

were accurate.

- Reviewed the DRGR system corrective actions for vulnerability scans to determine whether identified risks had been remediated.
- Evaluated applicable controls in the Federal Information System Controls Audit, NIST publications, and HUD's Information Technology Security Policy, 2400.25, REV-2, CHG-1.

INTERNAL CONTROLS

Internal control is a process adopted by those charged with governance and management, designed to provide reasonable assurance about the achievement of the organization's mission, goals, and objectives with regard to

- Effectiveness and efficiency of operations,
- Relevance and reliability of information, and
- Compliance with applicable laws and regulations.

Internal controls comprise the plans, policies, methods, and procedures used to meet the organization's mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations as well as the systems for measuring, reporting, and monitoring program performance.

Relevant Internal Controls

We determined that the following internal controls were relevant to our audit objective:

- Up-to-date written policies and procedures used for implementation of controls.
- Managerial oversight and monitoring.
- Compliance with Federal requirements.

We assessed the relevant controls identified above.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, the reasonable opportunity to prevent, detect, or correct (1) impairments to effectiveness or efficiency of operations, (2) misstatements in financial or performance information, or (3) violations of laws and regulations on a timely basis.

Deficiencies

Based on our review, we believe that the following items are deficiencies:

- [REDACTED] (finding 1).
- Application security management of the DRGR system had weaknesses (finding 2).

FOLLOW-UP ON PRIOR AUDITS

Review of Selected Controls Within the Disaster Recovery Grant Reporting System - Audit Report 2009-DP-0007

On September 30, 2009, the HUD Office of Inspector General (OIG) audited selected controls within the DRGR system (Audit Report 2009 DP 0007 - Review of Selected Controls Within the Disaster Recovery Grant Reporting System). The audit concluded that (1) access control policies and procedures for the DRGR system violated HUD policy, (2) the system authorization to operate was outdated and based upon inaccurate and untested documentation, (3) CPD did not adequately separate the DRGR system and security administration functions, and (4) CPD had not sufficiently tested interface transactions between the DRGR system and LOCCS. As a result, CPD could not ensure that only authorized users had access to the application, user access was limited to only the data that were necessary for users to complete their jobs, and users who no longer required access to the data in the system had their access removed.

In addition, the application had been operating under an outdated security certification for 7 months. Although CPD had initiated the authorization process, it was initiated without updated accurate documentation; therefore, results would also be based upon inaccurate information. To address the issues cited, OIG issued recommendations that CPD (1) formalize the user access request process and strengthen access controls; (2) update and correct system documentation and resubmit the revised documentation for security certification and accreditation; (3) separate the duties of system and security administration and reassign the help desk functionality; and (4) work with its contractors to ensure that tests of drawdown controls and transaction processing reports are performed as stated in the functional requirements documentation or if other controls are used, remove from the system documentation stated controls that are not in use.

CPD continued to address the recommendations through May 2011. Final actions to address the recommendations from this audit were taken, and all of the recommendations were closed as of May 31, 2011.

Appendix A

AUDITEE COMMENTS AND OIG'S EVALUATION

Ref to OIG Evaluation

Auditee Comments

OIG received CPD responses on July 8, 2011 via e-mail.

Comment 1

It is important to distinguish which data is critical [REDACTED]
[REDACTED] All financial disbursement requests from DRGR for funds to every organization under every HUD approved activity have always been submitted to LOCCS at the grant level and to be processed the grant banking information must match the Tax Identification Numbers (TINs) from our grantee/grant profiles to get to the bank routing info that is maintained by the HUD's CFO staff in Ft. Worth. No HUD or grantee users can modify any banking information in DRGR. If unauthorized users added activities, draws related to them would still go to the grantee bank accounts based on bank routing that is inaccessible from DRGR and any attempts to access these funds would still have to be done through the grantee's own financial systems.

Comment 2

Consequently, DRGR considers draw approvals paramount to tracking data on grantee oversight of money going to each funded organization. As previously explained to the OIG, many DRGR system actions taken by HUD staff and grantees each draw submission, approvals, rejections, and revision only occur once each [REDACTED] Each new action creates a new record with a user and a time stamp. [REDACTED]

[REDACTED] Other actions such as DRGR Action Plan and QPR report submission can also be archived [REDACTED]
[REDACTED] QPRs are typically only approved once and can only be unapproved by superusers which are tracked through email requests. CPD already tracks the comments of HUD staff reviews at the QPR level and at the activity level for every quarterly review of grantee such financial, performance, and program compliance issues [REDACTED]
[REDACTED]

As also discussed, system development work requests already existed before this OIG audit for modifying DRGR [REDACTED]
[REDACTED] CPD will use this work request to modify [REDACTED] key items related to user accounts. Rather than keeping only the latest record which can be easily archived, [REDACTED]
[REDACTED]

Ref to OIG Evaluation

Auditee Comments

Comment 3

However, beyond tracking activity drawdowns and obligation updates in addition to CPD comments at the activity level during every quarterly QPR review, CPD review of official grantee support records for compliance monitoring at the activity level occurs during on-site monitoring. Grantee information in DRGR is primarily used to facilitate risk assessments and to help determine the scope of on-site monitoring. HUD already modified DRGR to track every HUD action on grantee records using the grantee simulator under the last OIG DRGR audit. Responsibility for compliance with federal requirements is at the grantee level and repayment of any noncompliant use of funds is from the grantee. All controlled monitoring communications regarding non-compliance and any potential repayments are directed to grantee managers.

Comment 4

CPD does not agree that our goal should be to increase the # of total data elements tracked at the activity level through user, stamp and value changes. CPD considers the tracking excess grantee data elements at the activity level to have no value for audit and monitoring purposes. As explained above, DRGR already tracks key user audit information through archives. CPD already provided a detailed list of items to be modified in existing history tables during the field work portion of this OIG audit. We have spent a great deal of time and money recently tracking user certifications and improving system performance. Adding excess data elements would degrade system performance and responsiveness and serve no substantive monitoring/audit purpose.

Comment 5

[Redacted]	
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]

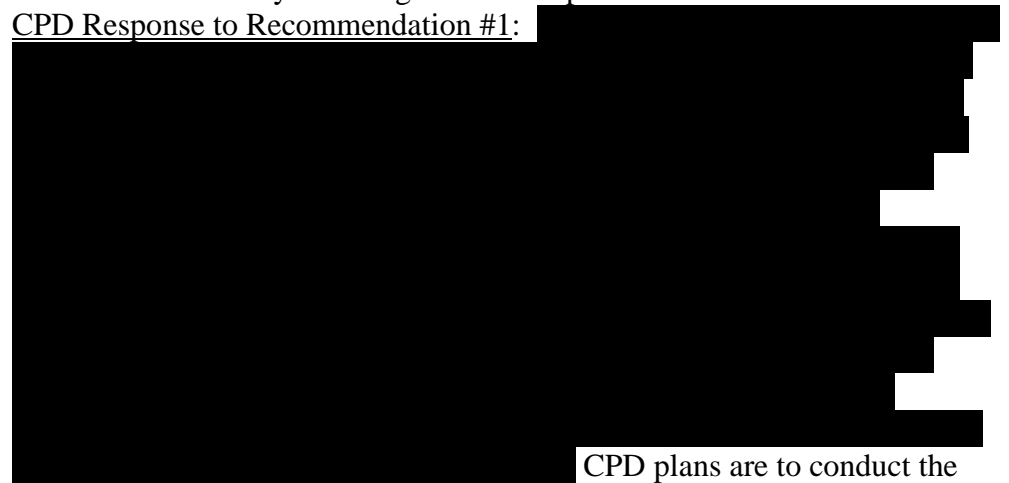
Comment 6

Cause #3 is not accurately stated. CPD and CISO staff conducted a DRGR Contingency Plan test on November 10, 2010 at 10:00 am. DRGR was declared a Mission Critical system October 6, 2010 and was updated as Mission Critical in CSAM; but did not get updated in HUD's Inventory of Automated Systems (IAS). The HUD IT contract for FY 2011 was already underway and DRGR did not get include in the scope of systems to be tested during the spring 2011 Disaster Recovery Testing

Office of Community Planning and Development:

CPD Response to Recommendation #1:

Comment 7

 CPD plans are to conduct the next DRGR Vulnerability Scan in July 2011, immediately following the next scheduled application release. As part of that process, the system owner and information system security officer and IT operations will verify that that all information security weaknesses identified in the 2009 DRGR scan have been remediated and will ensure that any newly identified weaknesses as a result of the scan are mitigated.

Comment 8

CPD Response to Recommendation #2: The DRGR system owner and its system security officers have updated the DRGR security documentation to consistently reflect DRGR's Status as mission critical and security categorization moderate in each document. The Contractor currently in the process of producing annual security documentation updates. CPD will ensure that the content of all future security documentation is consistent and reflects DRGR's current condition and status.

Comment 9

CPD Response to Recommendation #3: DRGR was declared a Mission Critical system in October 2010 and was updated as Mission Critical in CSAM. The system was not updated as mission critical in the HUD's Inventory of Automated Systems (IAS). Even so, the HUD IT contract for FY 2011 was already underway and did not foresee to include DRGR in the scope of the Disaster Recovery Testing). CPD coordinated with OCIO/Chief Information Security Officer (CISO) staff in October 2010 and arranged to have CISO staff conduct a DRGR Contingency Plan test on November 10, 2010 at 10:00 am. CPD will continue to coordinate with HUD OCIO and responsible contractors to conduct the contingency plan test on DRGR. CPD will also insure that ensure that HUD OCIO and responsible contractors include DRGR when performing DR tests.



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

CHIEF INFORMATION OFFICER

MEMORANDUM FOR: Hanh Do, Director, Information System Audit Division, GAA

FROM: Jerry E. Williams, Chief Information Officer, Q

SUBJECT: Draft Audit Report – The Disaster Recovery Grant Reporting System that Maintained Recovery Act Information had Application Security Control Deficiencies

This memorandum is in response to your June 29, 2011 draft audit report entitled, “The Disaster Recovery Grant Reporting System that Maintained Recovery Act Information had Application Security Control Deficiencies.”

The Office of the Chief Information Officer (OCIO) has carefully reviewed the report and is providing comments on the report and its recommendations. The attachment lists the recommendations issued by the Office of the Inspector General and OCIO’s response to the recommendations. Once the final report is issued, we will then be able to provide you with a definitive timeline and estimated completion date.

We look forward to working with you and your staff to resolve and close out the recommendations. Should you have any questions or need additional information, please contact Joyce M. Little, Director, Office of Investment Strategies Policy and Management, at 202-402-7404.

Attachment(s)

Comment 10

Comment 11

Comment 11

Draft Report Reference	Office of the Chief Information Officer (OCIO) and Management Comments for OIG’s Consideration
Page 13, Rec. 2A	Request the OIG revise the recommendation by deleting “IT operations” and replacing with “OCIO”.
Page 13, Rec. 2C	Request the OIG delete the recommendation in its entirety and replace with “Coordinate with the HUD OCIO to provide HUD Disaster Recovery Plan for Service Continuity and Availability Management (DRPSCAM) support for the DRGR system.
Page 13, Rec. 2D	Request the OIG delete the recommendation in its entirety and replace with “Ensure the DRGR system has HUD Disaster Recovery Plan for Service Continuity and Availability Management (DRPSCAM) support.”

OIG Evaluation of Auditee Comments

- Comment 1 CPD states that grantee users cannot modify banking information in DRGR, however this type of information was not reviewed in the scope of our audit. [REDACTED]
- Comment 2 After receiving documentation from the auditee prior to issuance of the draft report, OIG removed the following elements from the draft report; 1) create draws, 2) approve draws, 3) approve vouchers over threshold, and 4) approve quarterly performance reports.
- Comment 3 OIG disagrees that HUD has already modified DRGR to track every HUD action on grantee records. [REDACTED]
- Comment 4 OIG agrees with CPD that not all data elements need to be tracked. OIG has modified the draft report to reflect CPD comments received on specific data elements needed and not needed. The data elements that are listed in this report would serve monitoring and audit purposes in the event of a security violation.
- Comment 5 After receiving documentation from the auditee prior to issuance of the draft report, OIG removed data elements from the draft report. [REDACTED]
- Comment 6 The auditee is referring to “Cause #3” as written in the Notification of Findings and Recommendations that were provided on June 14, 2011. OIG disagrees that the cause is not accurately stated. On page 12 in the audit report, OIG states the cause occurred because system information was not entered into CSAM. CPD states that the system was not updated in IAS. OIG received confirmation from OCIO that information was not completely entered into CSAM. As a result, the cause will remain unchanged in the report.
- Comment 7 The auditee is referring to “Recommendation #1” as written in the Notification of Findings and Recommendations that were provided on June 14, 2011. This comment refers to recommendation 2A in the audit report. We acknowledge CPD’s response and are encouraged with their stated plan to address recommendation 2A.

- Comment 8 The auditee is referring to “Recommendation #2” as written in the Notification of Findings and Recommendations that were provided on June 14, 2011. This comment refers to recommendation 2B in the audit report. We acknowledge CPD’s response and are encouraged with their stated plan to address recommendation 2B.
- Comment 9 The auditee is referring to “Recommendation #3” as written in the Notification of Findings and Recommendations that were provided on June 14, 2011. This comment refers to recommendation 2C in the audit report. We acknowledge CPD’s response and are encouraged with their stated plan to address recommendation 2C.
- Comment 10 OIG agrees to revise the recommendation based on OCIO comments.
- Comment 11 OIG cannot revise the recommendation as suggested by OCIO. We did not review the HUD Disaster Recovery Plan for Service Continuity and Availability Management support for DRGR as it was not in the scope of our review. The plan was only mentioned after audit fieldwork was completed. We cannot determine whether the disaster test for DRGR will be included in the plan and how the test will be conducted for this mission critical system. As a result, the recommendation will remain unchanged in the report.