MIAMIBEACH

MEMORANDUM

City of Miami Beach, 1700 Convention Center Drive, Miami Beach, Florida 33139, www.miamibeachfl.gov
Office of Internal Audit
Tel: 305-673-7020

TO: Ana Salgueiro, Building Department Deputy Director

VIA: Mark Coolidge, Assistant Internal Auditor MDC

FROM: Norman Blaiotta, Senior Auditor

DATE: September 30, 2017

SUBJECT: **Assessment of Access Rights for EnerGov User Roles (Building Department)**

Meetings were held with the Building Permit Information Analyst to review and assess risks associated with created EnerGov user roles and the corresponding access rights and privileges granted to Building Department employees. A copy of the department's "EnerGov User Role Access Audit Report" is attached that details the access rights granted to pertinent staff as a result of these meetings.

The focus of this review was to identify instances whereby these user roles and/or corresponding system accesses granted could have an adverse impact on segregations of duties and/or internal controls. The thirty-four (34) EnerGov user roles listed below were created to grant access to the listed number of Building Department assigned users. The naming conventions were established by the Building Department in conjunction with the Information Technology Department so it was not changed to help avoid creating any confusion.

1 Bldg Admin Fin Sup – (1 user)
2 Bldg Admin Finance – (4 users)
3 Bldg Administrative – (2 users)
4 Bldg Chief Code Comp Off – (1 user)
5 Bldg Chief Elec Inspector – (1 user)
6 Bldg Chief Mech Inspector – (1 user)
7 Bldg Chief Plum Inspector – (1 user)
8 Bldg Chief Roof Inspector – (1 user)
9 Bldg Chief Struc Engineer – (4 users)
10 Bldg Code Compl Admin – (2 users)
11 Bldg Code Compl Clerk – (2 users)
12 Bldg Code Compl Off – (2 users)
13 Bldg Elec Inspector – (2 users)
14 Bldg FOG Dischrg Ctrl Eng – (1 user)
15 Bldg Gov Compliance Off – (1 user)
16 Bldg Insp Admin – (1 user)
17 Bldg Insp Clerk – (6 users)
18 Bldg Mech Inspector – (1 user)
19 Bldg Official Admin Aide – (2 users)
20 Bldg Official – (4 users)
21 Bldg Permit Clerk I – (14 users)
22 Bldg Permit Clerk II – (5 users)
23 Bldg Plum Inspector – (1 user)
24 Bldg Records Clerk – (3 users)
25 Bldg Records Supervisor – (2 users)
26 Bldg Senior Bldg Insp – (12 users)
27 Bldg Senior Bldg Insp – (2 users)
28 Bldg Senior Plum Insp – (3 users)
29 Bldg Sr Bldg Insp Sup – (1 user)
30 Bldg Sr Bldg/Code Officer – (1 user)
31 Bldg Sr Bldg/Roof Insp – (2 users)
32 Bldg Sr Elec Insp Sup – (3 users)
33 Bldg Sr Mech Insp Sup – (1 user)
34 Bldg Sr Plum Insp Sup– (2 users)

The following fifteen additional user roles were also created but have no individuals assigned and therefore should be deleted:

1. Bldg-StdWF-INSUP-PR-Hold
2. Bldg-StdWF-Holds
3. Bldg-Std-WF-Fee-INSUP-VIO
4. Bldg-StdWF-FeeAdm-PermSup
5. Bldg-Std,WF-FeeAd-PR-INSP
6. Bldg-Std User, WF Admin
7. Bldg-Standard, INSP Supv
8. Bldg-Router-WFA-INSUP-PR
9. Bldg Senior Elec Insp
10. Bldg Plan Review Admin
11. Bldg Permit Admin
12. Bldg Official Admin
13. Bldg Customer Serv Clerk
14. Bldg Chief Mech Inspector[1]
15. Bldg Build Inspector

Only one (1) user role can be assigned to each staff member; however, all employees assigned under a user role will share the same system accesses and privileges. In other words, department users have a one-to-one relationship with user roles, while user roles have a one-to-many relationship with department users.

After reviewing the access rights and privileges granted to each of the thirty-four (34) pertinent EnerGov user roles, it was noted that the following items are in need of further consideration, which have been highlighted on the User Role Access Reports presented after this memo.

1. All thirty-four (34) user roles were granted the ability to manage work flows through two (2) distinct rights, "AllowWorkflowManagement" and "WorkFlowAdministrator". The first right allows users to bypass steps or actions in the workflow for a particular record, as well as create steps and actions in a pre-established workflow. The second right allows users to create, delete, alter and approve workflows. Although a report can be generated to identify all instances in which a workflow step was bypassed, it would require continuous monitoring to detect any incidents whereby a step or an action is skipped or approved through the workflow.

   Best practices would be to map out the current business processes so that creating the workflow is easier and each required step or action is given the adequate hierarchy in the workflow; therefore, removing the need to allow access to any user role to manage the workflow. Workflow management should be a procedural control and not an operational option. Consequently, Internal Audit recommends ensuring that workflows are created to reflect the processes of the department and once properly set up that only System Administrator level users should have access to manage or administer workflows. Workflows should be the result of Standard Operating Procedures and established business rules within the department.

   Furthermore, according to EnerGov's User Setup Manual (Exhibit A), under "Security Functionality" (p. 5) the function of a System Administrator is defined as "Allows the user to perform the same functions as Allow Workflow Administrator". By definition, System Administrator is the most comprehensive access right in any system so that anyone granted the Allow Workflow Administrator access has in fact a System Administrator access role.

1 - There are two roles named exactly the same (Bldg Chief Mech Inspector) but only one has personnel assigned to it.

For this reason, it is recommended to remove these rights from everyone but the actual System Administrator.

2. The rights shown below in Table 1 were granted to non-managerial personnel and provide each assigned user with a high level of discretionary control over transactions. If it is imperative for these user roles to have the listed rights, then adequate internal controls and departmental processes should be established to ensure a proactive monitoring process to detect any errors, unnecessary or insufficiently documented transactions, etc.

   Also, departmental management should determine if the right to delete fees is necessary since they often may be adjusted without the need to be deleted. However, if management believes that the need to delete fees is necessary for their course of business, the adequate processes and controls should be implemented procedurally to detect and/or avoid errors and/or unauthorized deletions.

Table 1

Rights	Roles	Rights	Roles
AllowAdjustFees	Bldg CodeCompl Admin Bldg Code Compl Clerk Bldg Code Compl Off Bldg Insp Admin Bldg Official Admin Aide Bldg Permit Clerk I Bldg Permit Clerk II	**AllowDeleteFees**	Bldg CodeCompl Admin Bldg Code Compl Clerk Bldg Code Compl Off Bldg Insp Admin Bldg Official Admin Aide Bldg Permit Clerk I Bldg Permit Clerk II
AllowInvoiceEditing	Bldg CodeCompl Admin Bldg Code Compl Clerk Bldg Code Compl Off Bldg Insp Admin Bldg Official Admin Aide Bldg Permit Clerk I Bldg Permit Clerk II	**AllowVoidInvoices**	Bldg CodeCompl Admin Bldg Code Compl Clerk Bldg Code Compl Off Bldg Insp Admin Bldg Official Admin Aide Bldg Permit Clerk I Bldg Permit Clerk II
AllowDeleteAttachment	Bldg CodeCompl Admin Bldg Code Compl Clerk Bldg Code Compl Off Bldg Insp Admin Bldg Official Admin Aide Bldg Permit Clerk I Bldg Permit Clerk II Bldg Senior Plum Insp Bldg Sr Bldg/Code Officer	**AllowVoidPayments**	Bldg CodeCompl Admin

F:\OBPI\$AUD\INTERNAL AUDIT FILES\DOC16-17\PC WORK\EnerGov Roles & Rights\Buildings - 7-20-17\Audit Memo EnerGov Roles and Rights -Building Department 09-30-17 2.docx

cc: Susanne Torriente, Assistant City Manager
Mark Taxis, Assistant City Manager
John Woodruff, Chief Financial Officer
Ariel Sosa, Director – Information Technology Department