City of Milwaukee

Office of the Comptroller

W. Martin Morics, C.P.A.
Comptroller

Michael J. Daun
Deputy Comptroller

John M. Egan, C.P.A.
Special Deputy Comptroller

Craig D. Kammholz
Special Deputy Comptroller

December 22, 2010

To the Honorable Common Council
City of Milwaukee

RE: IT Firewall Audit

Dear Council Members:

As a component of the Comptroller's comprehensive information systems audit work plan, the firewall audit was conducted from August to November of 2010 and involved the review of a sampled number of firewall rule and route configurations (firewall rules and routes govern how various data enters and leaves the City's computing environment). The audit consisted of the comprehensive review of six firewalls, including the Municipal Court firewall, Department of Public Works firewall, Water Department firewall, Health Department firewall, Information Technology Management Division firewall and the PeopleSoft FMIS firewall.

Proper firewall configurations are an important and tangible part of ensuring that the City's computer systems are available and that City services connected to computing resources are not impaired. A firewall must therefore maintain high standards for assuring the secuirty, integrity and functionality of the computer environment.

As recently as 2009 City divisions managed their own firewalls internally. This resulted in the use of various firewall hardware and software being used throughout the City. No single configuration security standard was used by all City divisions to configure and manage their firewall settings. In the first quarter of 2010 most City firewalls were centeralized under the Department of Public Works and are now controlled and managed by DPW. The exceptions to this centralization initiative are; the Port of Milwaukee firewall, Employes Retirment System firewall, Police Open Sky firewall and Library firewall. DPW now uses a single standard software to manage all ten firewalls for which they are responsible.

When firewall management responsibilities were centralized DPW inherited the existing configuration rule sets and routes into their firewall management software. This centralization also resulted in a significant information system infrastructure change to update servers and networking equipment. With so much change being introduced into the security layer of the City's network many firewall rules and routes have become either redundant or obsolete.

Firewalls were evaluated for IS industry standard firewall configuration and firewall governance controls. These standards include:

- Firewall configuration and maintenance is governed by a written firewall policy.
- Firewall access management screens are limited to appropriate management personnel through a limited security group.
- Firewall rules and routes are enforced in a logical hierarchy.
- Firewall rules and routes are current and efficiently configured.
- Firewall rule sets are completed with an "Any-Any Deny" rule to protect against unknown communication. This rule states that any communication method not defined by previous firewall rules is not allowed access.
- Firewalls are enabled with traffic activity logging for detective purposes, should an adverse event be detected.
- Firewall settings are regularly backed up on external media for disaster recovery purposes.
- A formal process is in place to request and enact firewall rule changes and maintain efficient firewall configurations.

The Comptroller's Senior IS Auditor, DPW Telecommunication Project Leader, and various firewall owners met weekly and reviewed the sampled firewalls for adherence to the above industry standards and came to a conclusion on each of these criteria.

The audit indicates that the DPW managed firewall rules were somewhat outdated but did not present a security risk. Firewall configurations that were obsolete or unnecessary were immediately disabled or removed during the audit. The Senior IS auditor identified several exceptions as a result of this audit and recommendations for improvement have been communicated to the appropriate City personnel.

Firewall configuration and maintenance is not governed by a formal firewall policy. However it is evident that the DPW managed firewalls are configured and managed using standards of efficiency and uniform logic. In each of the firewalls sampled access to firewall management screens were limited to appropriate management personnel through a limited security group. The administrative users included the DPW network infrastructure team members who actively manage the firewalls and respective business owners of the firewalls like departmental information systems staff.

It was determined that firewall rules and routes are enforced in a logical hierarchy. However, many of the firewall rule sets were not current and were inefficiently configured due to the inheritance of partly outdated rule sets. About 20 percent of rules were deemed outdated or irrelevant by firewall owners and firewall management. These rules were removed or updated during the audit as they were identified. All firewall rule sets that were examined were completed by the "Any-Any

Deny" rule to protect the City's network against unknown communications. The audit determined that network traffic activity logging is enabled on all firewalls for detective purposes should an adverse event be detected. Firewall settings are also backed up daily through an automated process and backup media is taken offsite once a week for disaster recovery purposes.

While an established communication channel and process are in place to request and enact firewall rule changes and maintain efficient firewall configurations this process is not formally documented. This means that firewall owners (various divisions) and firewall managers (DPW network infrastructure team) have not formalized what their responsibilities are regarding firewall management.

1. **Firewall configuration, maintenance and change management processes are not governed by a formal firewall policy.**

Recommendation: DPW network infrastructure management should consider authoring a formal firewall policy which would outline their configuration best practices, maintenance responsibilities and the formal rule change request process.

2. **All 6 sampled firewalls were found to have several antiquated rules and routes but were immediately updated.**

Recommendation: The remaining 4 DPW managed firewalls should be reviewed and updated. All firewall configurations should be evaluated at least once a year or as soon as possible after a large IS infrastructure changes.

3. **Many firewall rules were not notated as to their purpose in the firewall management software. This can cause confusion in future configurations.**

Recommendation: All firewall rules and routes should be notated in the "comments" column of the firewall management module.

All City Employees who participated in this audit should be commended for their availability and cooperation throughout the firewall audit process. The Comptroller thanks all parties involved in this audit for their enthusiastic cooperation with the auditor.

Sincerely,

for W. MARTIN MORICS
Comptroller

CC: All Division heads of audited departments
Nancy Olson, CIO
Jeffrey Mantes, DPW Commissioner