Security remarks to F&P Oct. 18, 2006
Randy Gschwind, Chief Information Officer

Good morning, Aldermen. I have talked to you twice before about information security since the Comptroller's security audit was released in April of 2005.

In July of 2005, I told you that there were real security threats out there, but that they are addressable through a coordinated program to address security in IT. This is achievable if we can understand where we are now, and plan where we need to go to reduce information security threats. We continuously attempt to gather information about where we are now so we can plan for the future with regard to information security. This is easier for some departments than for others, but we are making progress by working together.

Second, I told you that we needed to address quick hits that could improve security. Lacking any new resources, we have addressed some of these, but not enough. For example, the results of the original audit were provided to the departments who participated, but we are not aware that any follow-up was done to assess what measures were taken to address the identified security issues.

Third, I told you that we needed to review and update citywide information policies and procedures. That process has begun and will result in better and more relevant policies, but we also need to create greater awareness at the department and employee level. Security is only as good as each employee makes it.

Fourth, I suggested that we needed a security architecture for the whole City, rather than individualistic and uncoordinated approaches, but given the decentralized nature of IT in the City, this has been difficult to advance. We will continue to work with departments at a cooperative level to at least share information and approaches.

In February of this year, I enumerated for you the approaches and solutions we were undertaking to improve security in the City organization. These included:

- Adoption of an Information Technology Strategic Plan by the Citywide Information Management Committee and the Common Council. Security is an integral part of this plan.
- Changing the City code in 2004, providing the CIO with more authority to oversee and manage citywide initiatives such as security.
- Creating a single citywide e-mail system. This project is well underway.
- Working with DPW to create an MOU for management and operation of the extensive City of Milwaukee information network. The MOU is in place.
- Inventories of hardware and software across the City, so that standards can be implemented that will make these platforms easier to secure.
- Server consolidation at ITMD, reducing the number of servers and improving physical security, and backup and recovery procedures.

- Disaster recovery plans for all departments who operate their own data centers. This is now being approached as part of the overall COOP/COG process, and we are making progress.
- Improving communication and employee awareness. We have started to place security information on the MINT. In addition, ITMD has started the process of facilitating a citywide team of "Information Security Officers" from departments who will share information and formulate best practices in the area of security.

Finally, I have told you that staffing and resources for security are an issue. We have created security staffing in ITMD by assigning existing staff to this area, and we are making progress. As we try to bring more efficiency and improved effectiveness to information systems in the City, we will need to realign City IT funding to focus more resources on coordination and control at a citywide level for things like security, while not hindering departmental management of their applications and data. This will be a careful but necessary balancing act.

We will continue to work with departments and the budget office to focus necessary resources on security. While improvements have been made, much remains to be done. Among these are:

- Improved employee security training and awareness
- Ongoing analysis of vulnerabilities and the means to monitor and address them
- Better security coordination among our decentralized IT silos
- Standardizing security approaches across the City of Milwaukee
- IT disaster recovery plans for all departments
- Hardware, software, data and systems development standards
- Better change control management
- Continued systems and server consolidation

We have a long way to go, but at least have started the journey. I am happy to answer any questions you may have.