Security address to F&P Feb. 23, 2006
Randy Gschwind, Chief Information Officer

I last reported on security before this committee on July 21, 2005. At that time I told you that the City has real IT security issues that need to be addressed, as revealed partially in the Comptroller's security audit that was released in April of 2005. My recommendations were that the City needed to:

- Understand the current situation - what and where are the City's IT assets and how are they configured to make them secure?
- Address quick hits – security issues that can be remedied quickly and most easily.
- Update security policies and procedures, and make sure they are communicated and understood by all City staff.
- Standardize approaches to IT to improve overall security and control.

Some of this has been started, but much remains to be done. The security audit identified problems in numerous areas, and recommended:

- Developing an information security improvement plan and security architecture model
- Correcting the most urgent vulnerabilities
- Centralizing information security in DOA, and implementing common security tools and methodologies
- Creating an Information Security Officer position in DOA
- Fully implementing the risk assessment recommendations
- Performing ongoing security assessments

Security is an ongoing and critical issue for any large enterprise that relies heavily on IT and communications. Our IT is highly decentralized across multiple departments, and each one will tell you that they are secure, but there are always weak links and those become our vulnerabilities at the enterprise level. We will only address this by working together at an enterprise level, not each doing our own thing and hoping for the best. We must transform the individual security of departments into the collective security of the entire City, while still allowing for effective data sharing and efficient communications.

The IT consolidation ordinance that you passed last March provides the CIO with the authority to create standards, monitor and enforce best practices. Security is a critical area in which we need enterprise-wide policies and standards. So what has been done in the area of security?

First, a Citywide "Information Technology Strategic Plan" has been completed and adopted by the CIMC. This plan sets specific objectives and strategies in the area of security, including:

- Identifying risks
- Ensuring user awareness
- Creating a safe infrastructure

- Eliminating points of vulnerability
- Implementing best practice policies, procedures and standards

We are developing specific actions to implement these objectives, which will be rolled out over the course of this year.

Secondly, the IT ordinance which you passed last year has resulted in initiatives that will improve security through consolidation. An inter-departmental team met over the course of 5 months last year to choose a single e-mail system for the entire City. This will be implemented in ITMD over the next 6-9 months, and will increase efficiency and security, not to mention that your e-mails will now get delivered to the department you sent them to.

Part of the preparations for this single citywide e-mail system requires departments to participate in a system called Active Directory. Active Directory will help network security by allowing users to have a "single sign-on" to access network resources. Active Directory has many built-in security features like security auditing, administrative templates, and Group Policies. Administrative templates are used to determine when the passwords expire, force users to have complex passwords, and many other security options. The Group Policies are used to lock down/secure the servers, workstations, and Active Directory objects. Our network environment will become more secure.

Third, we are working to develop the capacity for DPW to manage and operate all the City's network elements, in coordination with DOA. Last year we worked together to create a Network Management MOU that specifies the performance areas that DPW is responsible for. This year we will work with them to develop a citywide plan for network management, operations and policies.

Fourth, the Director of Business Operations and I have asked all City departments to prepare an inventory of desktop equipment. This is being compiled at the present time, and will be used to analyze and standardize the City's approach to desktop hardware and software, which will aid in applying common security practices and procedures across all levels of the organization.

Fifth, ITMD has begun to consolidate some servers from disparate department locations into our secure and environmentally controlled data center in the 809 building. This improves the physical security of the infrastructure, as well as ensuring regular backup of data and maintenance of operating systems to current standards, which decreases the probability of failure or a security breach. We need to ensure that all separate department systems have similar procedures in place.

Sixth, in ITMD we back up all data and systems and send the backups weekly to a secure storage location at least 5 miles from City Hall. ITMD also has a written disaster recovery plan for our data center and the systems it contains. We need to require these from all City departments with their own systems and data centers. The former MIPC directed all departments to do this in late 2002, but only two responded. I will bring this issue back to the CIMC next week for direction to departments to prepare IT disaster recovery plans.

Seventh, I have asked some of my staff to study security issues and develop recommendations for addressing issues with current staffing and resources. We also involved the Comptroller's audit staff and the Water Works Security Manager in these meetings. Current recommendations include improving communication with departments and getting buy-in to security principles, training programs for staff and employees, and development of standards and guidelines. Employee awareness is key, since this is not just a technical problem. An area will be created on the MINT for best practices information.

Finally, staffing and resources for security are an issue. There is currently no explicit security function or staffing in ITMD. Therefore, development of policies and standards, monitoring and enforcement are issues that have to be dealt with as "other duties as assigned." 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 difficult but necessary balancing act.

In summary, ITMD has responded positively in many areas to security threats, working to create disaster recovery plans, implementing anti-virus software, applying software patches, doing regular backups of critical information (and storing those backups offsite), installing firewalls, addressing internal security threats, and securing physical facilities. However, to paraphrase the old maxim, fragile links remain that continue to weaken the city's chain of defense against security risks. Uncoordinated security-related efforts by city departments leave areas of vulnerability that — because of the interrelated nature of information systems — jeopardizes the city's overall security. Moreover, lack of training and systems for disseminating information about imminent threats compromises the most important link in the chain: users. We will work to improve security and reallocate resources in this direction in the future.

I'd be happy to answer any questions you may have.