Common Council File

City of Milwaukee Information Technology Security Risk Assessment

W. MARTIN MORICS
City Comptroller
City of Milwaukee, Wisconsin

April 2005

Table of Contents

City of Milwaukee

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

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

Michael J. Daun
Special Deputy Comptroller

Office of the Comptroller
April 20, 2005

To the Honorable
the Common Council
City of Milwaukee

Dear Council Members:

We engaged the consulting firm Jefferson Wells International to conduct a security risk assessment, from the period December 2003 through June 2004, of the computer networks used by ten major City departments. Attached are our comments on this risk assessment, followed by the Jefferson Wells Security Risk Assessment Report.

The risk assessment found that some City departments have taken positive steps toward securing their respective computer networks. Nevertheless, serious security vulnerabilities were identified. Certain of these vulnerabilities are of a critical nature, potentially compromising essential City services. Since City department computer networks are connected to each other and to the Internet, security vulnerabilities in individual departments could affect other departments. These interconnected networks require a consistent Citywide approach to security.

We recommend that critical vulnerabilities identified by Jefferson Wells be corrected as soon as possible and that the overall state of computer security be improved by establishing a centralized information security oversight function.

Appreciation is expressed to City departments for their assistance in conducting this network security risk assessment.

Sincerely,

W. MARTIN MORICS
Comptroller

I Objectives and Scope

On May 9, 2002 the Chief Information Officer (CIO) for the City of Milwaukee wrote the Comptroller recommending that an audit be conducted of computer network security. The CIO stated that *"...the City has a very decentralized information technology [computer] architecture with many different types of hardware and software, interfaces and other exposures to outside agencies and facilities – most of these are not under the umbrella of the DOA-ITMD security infrastructure [Information and Technology Management Division of the Department of Administration] ...the City of Milwaukee IT network is a connected conglomeration of departmentally managed pieces. We believe that the security of such an interconnected shared infrastructure is only as strong as the weakest link. Therefore, each of the department pieces needs to be examined..."*

In 2003 the Office of the Comptroller engaged the consulting firm Jefferson Wells International to conduct a security risk assessment of City of Milwaukee information technology (IT). The primary objective was to conduct a high-level evaluation of the security practices and processes used to protect the confidentiality, integrity, and availability of City information assets. An additional objective was to identify potential future information security audits. The appended Security Risk Assessment Report by Jefferson Wells meets these objectives. The Office of the Comptroller will utilize the *"IT Audit 'Roadmap'"* at the end of the Jefferson Wells Report for planning future information security audits.

The scope of this risk assessment was limited to the following ten City departments and divisions with major information technology operations:

1) City Clerk
2) Department of Administration – Information & Technology Management Division
3) Department of City Development
4) Department of Public Works
5) Employes' Retirement System
6) Health Department
7) Milwaukee Fire Department
8) Milwaukee Public Library
9) Municipal Court
10) Milwaukee Water Works

Jefferson Wells obtained documentation from these departments on computer hardware, software and networking infrastructure, interviewed department staff, and scanned department networks using a software application that identified security vulnerabilities. Department specific information on security vulnerabilities was provided to staff in each of the departments.

Originally the Milwaukee Police Department (MPD) was to be included in the security risk assessment. However, the risk assessment could not be conducted on Police systems because MPD would not allow any documentation about its systems to leave the department. MPD indicated that security could be jeopardized if documentation on its systems were maintained outside the department. Therefore, the security of MPD computer systems was not reviewed. Similar concerns were expressed by some of the other departments, but the Office of the Comptroller was generally able to work through those concerns. For example, the Milwaukee Fire Department provided limited documentation and no interviews, but allowed its networks to be scanned and the scan results documented. Also, the Milwaukee Water Works provided documentation and allowed its department network to be scanned, but did not allow its water control system to be scanned.

II Organization and Fiscal Impact

In that IT has become essential for the delivery of many City services, City departments have integrated information technology into their core business practices. The life-line communication and dispatching systems for Police and Fire depend on City IT. Citizen ballots are processed electronically with IT. The Health Department is connected to other public health agencies over the Internet. The Water Department uses IT to monitor and control water plant equipment. The Treasurer and the Employes' Retirement System move City funds electronically between financial institutions over the Internet. All City accounting and payroll transactions are now processed remotely over the Internet.

As noted by the City's CIO, responsibility for City information technology is decentralized. City departments operate their own computer networks that connect computers within a department for communication and sharing of business applications, data files and resources such as printers. To a greater or lesser extent, individual departments retain their own computer staff to support their networks and business applications.

These department networks, known as Local Area Networks (LANs), are interconnected to form the City's Wide Area Network (WAN), making interdepartmental communication and file sharing possible. The Department of Public Works constructed and maintains the City's WAN infrastructure, consisting of fiber optic and copper cabling in underground conduits, along with networking hardware and software. DPW provides the Internet connections used by most City departments. DPW also provides network support to Police, Fire, Water Works, Health, Department of Neighborhood Services, Library, Port, and Municipal Court. The Department of Administration provides network support to the other departments, generally located in City Hall. However, in this decentralized IT management environment, there is no single City agency providing guidance and oversight over the acquisition, installation, maintenance and use of City IT resources. For example, auditors were unable to find a consolidated Citywide inventory of IT equipment and networking infrastructure. The Department of Administration could not provide the auditors with information on the total number and extent of Local Area Networks, applications, databases, backup facilities, web-servers, desktop workstations, etc. currently operating in City government.

As mentioned above, many City government functions are dependent on computer networks and related databases. The City Wide Area Network extends to access locations throughout the City. Hundreds of thousands of electronic communications and transactions occur daily within City government and between City government and vendors, residents and other organizations. These range from emergency dispatch of police and fire units to the recently implemented electronic payment of property tax bills. Such basic City government functions are subject to the continuous threat of delay or failure due to the destruction or corruption of the related computer networks and databases. Problems could result from unintentional errors or intentional efforts to disrupt City systems. Therefore, the City of Milwaukee must have in place effective information security policies, systems and procedures to prevent or otherwise minimize damage from breaches in computer security.

Information technology is not only essential, but also a costly City resource. The Department of Administration indicates that the cost of City information technology increased 64 percent between 2000 and 2003. The Exhibit 1 budget summary prepared by DOA shows that for 2004, the City budgeted $40.1 million for IT. These budgets cover the personnel, equipment and services related to City department computer networks and the development and maintenance of the applications running on those networks. This total also includes major new IT systems for the Milwaukee Police Department, Milwaukee Fire Department and Employes' Retirement System. The Department of Public Works indicates that Exhibit 1 also includes staff support for the City telephone systems.

III Network Security Risk Assessment

The risk assessment found that some City departments have taken positive steps toward securing their respective IT networks. Nevertheless, serious security vulnerabilities were identified. These vulnerabilities could lead to the loss or corruption of City data, interruptions in City services, and financial loss to City government.

A. Current Security Strengths

The security risk assessment found that City departments are generally aware of the need to protect their respective computer systems from unauthorized access. Several departments expressed appreciation for the information disclosed by the risk assessment. This positive attitude about security is a significant strength.

The Jefferson Wells Security Risk Assessment Report notes that *"...several of the departments/divisions appeared to have reasonable security controls and had formal department/division level security policies and procedures. It was observed that City department/division managers and their respective IT representatives were generally aware of the implications of the control questionnaires and security comments discussed by Jefferson Wells personnel and, that City personnel demonstrated an interest to maintain and/or strengthen their current security controls."*

B. Current Security Vulnerabilities

1) Serious Information Security Risks Exist

Despite these security strengths, the Jefferson Wells Report concludes that *"The overall state of risk the City faces in regards to information security is considered serious."*

Security vulnerabilities noted in the Jefferson Wells Report are summarized in Exhibit 2. **Thirty seven vulnerabilities were found in one or more of the nine City departments interviewed.** Some departments had inadequately secured Internet connections. Some departments had inadequately managed "firewalls", used for controlling access across network perimeters. Some departments had inadequate password controls. One department had inadequate anti-virus protection. During July 2004 each department reviewed, including the Departments of Administration and Public Works, received detailed information on the security vulnerabilities identified by Jefferson Wells. A Network Vulnerability Assessment Report generated by the network scanning software was provided to each department.

Both the City CIO and Jefferson Wells have indicated that information security in the City overall is only as strong as the "weakest link". **The above weak links therefore potentially endanger the continued operation of all City information technology processes.**

The Jefferson Wells Security Risk Assessment Report identifies the following managerial deficiencies that appear to be behind many of these security vulnerabilities:

- *"Lack of planning related to centralized/decentralized security programs and lack of governance over security initiatives and controls*
- *Lack of current security self-assessments and awareness efforts*
- *Lack of enforcement of security policies, procedures, and solutions used with managing access to City information assets*
- *Lack of enforced standards for technical configurations and business processes that reduce and/or prevent security risks*
- *Inadequate citywide monitoring programs in place to detect security risks and report weaknesses*

- *Lack of centralized solutions to track and resolve potential security risks and/or problems on a timely basis"*

City information security vulnerabilities have at times been exploited. In June 2004 the City was informed that a City department business web-server[1] had been hijacked for criminal purposes. An unauthorized web-page had been installed on the City web-server to solicit credit card information under the guise of a Brazilian bank. Upon discovery, the City disconnected the web-page from the Internet and contacted the Federal Bureau of Investigation. The unauthorized web-page had been installed on the inadequately secured City server over the Internet. Ultimately, there was no indication that City data or IT operations had been jeopardized in this instance. However, City IT resources were used in an attempt to defraud the Brazilian bank's customers. The Department of Administration indicated that this City web-server has since been secured. This event underscores the urgent need to address the deficiencies noted by Jefferson Wells.

2) Decentralized IT Impedes Security

When the City began to use information technology in the late 1960s, computer processing was accomplished with centrally located mainframe computers. The Central Electronic Data Services Department (CEDS) was created to provide IT services to City departments. CEDS controlled most of the computer equipment, software and technical computer personnel. As computer processing moved to the users' desktop, CEDS had difficulty providing the on-site and real-time technical assistance needed by City departments.

According to the Department of Administration, the City's decentralized information technology governance began in 1992 with the creation of the Internal Service Improvement Project. Under this approach City departments were given budgetary control over IT and the ability to choose their IT vendors. CEDS was restructured into the Information Systems Division (ISD) of the Department of Administration, with the objective of making the division more efficient and competitive in the delivery of IT services. Individual City departments often chose to exercise their independence by acquiring their own computer hardware and software, hiring their own IT support staff and contracting with outside vendors rather than ISD. While this decentralized IT environment promotes individual department accountability and flexibility, it makes the application of a consistent set of information security requirements difficult.

The City has undertaken several initiatives to improve information security in this decentralized environment.

In 1995 the Milwaukee Information Policy Committee (MIPC) was established by Milwaukee Code of Ordinance Chapter 320-31 to *"Formulate public policy guidelines concerning electronic information that deal with its access, use, documentation, integration, sale, distribution, security and related issues..."* In 1996 the MIPC issued a set of security guidelines in a document titled Information Systems Management Policy Guidelines, intended in part *"...to safeguard the integrity, availability, viability, and security of the electronic information resources of the City..."* City Ordinance Chapter 320-31 was amended in 2004, replacing the MIPC with a new City Information Management Committee. Like its predecessor, this new committee is to propose policies to the Mayor and Common Council for the management of the City's information resources, including security.

In 1996 the Department of Administration issued Information Security Policies and Standards, which address many aspects of information technology risk assessment and security management. According to Jefferson Wells, six of the nine departments it interviewed for this security risk assessment were not following these 1996 guidelines, including four departments that were unaware of the existence of such guidelines.

In 2000 ISD was again restructured into the Information and Technology Management Division (ITMD) of the Department of Administration. The 2000 budget states that *"This division will oversee information and telecommunications policy development...coordinate departmental information systems, evaluate requests for technology improvements, and maintain existing infrastructure systems, including 'CityNet', the City's wide area network..."* Also, in 2000 the City created the Chief Information Officer (CIO) position to head ITMD.

These initiatives have so far been unsuccessful in materially reducing information security vulnerabilities. This may have occurred in part because City ordinances did not

[1] A "server" is a computer device attached to a network that provides applications and other resources to the network. A "web-server" provides Internet accessible web-pages.

provide a sufficient foundation for effective Citywide governance of information technology and related information security, or sufficient enforcement authority.

Ordinance Chapter 310-1 simply stated that the Department of Administration is responsible for information and technology management, without specifying what this responsibility entails or providing any authority to execute such responsibility on a City government-wide basis. Further complicating information technology governance, is Ordinance Chapter 309-1 which stated that the Department of Public Works is responsible for all matters relating to municipal communications. DPW thereby maintained that it had some responsibility for managing City IT, since the City Wide Area Network requires the installation and maintenance of a communications infrastructure. These ordinances did not clarify the potentially conflicting roles of these departments or other City departments in IT management. Further, DOA and DPW generally have not coordinated their IT management and security efforts effectively.

Both the City CIO and Jefferson Wells state that a consistent City government-wide approach to information security is needed, but that the current decentralized IT environment makes this difficult to achieve. Jefferson Wells reports that *"...the decentralization and lack of citywide governing controls will continue to hinder the City from creating a secure, interconnected environment. We highly recommend that the City evaluate the effectiveness of the current decentralized network environment and consider addressing information security controls on a timely basis from a centralized, citywide, point of view."*

Many day-to-day IT decisions made by City departments acting without Citywide guidance often lead to future problems and added costs. IT systems developed by user departments often become more difficult to expand or change because trained City computer programmers are not on staff for the programming language of the software purchased. Quantity discounts may be missed as individual departments are unaware of similar hardware needs in other departments. Automated communication and data sharing between department systems can be made difficult or impossible because these needs were not considered with the initial department's system implementation.

Moreover, as it relates to computer security, Jefferson Wells concludes that these stand-alone IT decisions may leave City departments with inadequate computer security and a Citywide data processing environment vulnerable to breach and potential system failure.

The City is not alone in facing information security obstacles related to a decentralized environment. The United States Government Accountability Office, formerly the General Accounting Office, reported in 1998 that *"...in our reports over the last several years, we have made dozens of specific recommendations to individual agencies. Although many of these recommendations have been implemented, similar weaknesses continue to surface because agencies have not implemented a management framework for overseeing information security on an agency wide and ongoing basis."* [2]

The Mayor recently announced a new initiative to better coordinate information technology governance and to *"Establish a more unified governance structure that provides a strategic direction for IT, better control of IT costs, improved coordination of IT efforts, better integration and access to information."*[3]

In response to this initiative, the Common Council recently revised City ordinances to assign the responsibility for coordinating IT policy and management to the Department of Administration through its CIO. The City Information Management Committee is to provide advisory assistance to the CIO in the development of IT policies, plans and standards.

The City should benefit greatly from the changes in information technology governance called for by these revised ordinances. Ultimate success will depend upon full implementation by the Department of Administration. Active and cooperative participation by the Department of Public Works and other major City departments is essential. Also, establishing and enforcing Citywide IT policies, plans and standards will make it easier to improve City information security.

C. Recommendations

As previously noted, Jefferson Wells found a *"Lack of planning related to centralized/decentralized security programs...Lack of enforcement of security policies...Lack of enforced standards for technical configurations...Inadequate citywide*

[2] GAO Accounting and information Management Division May 1998 Executive Guide Information Security Management Learning From Leading Organizations

[3] The Mayor's January 28, 2005 presentation to City departments titled Improving Information Technology Management in Milwaukee

monitoring...Lack of centralized solutions..." The Jefferson Wells Security Risk Assessment Report (See Appendix) recommends the following four new major initiatives to improve the City's information security program, together with thirty seven specific actions to reduce the vulnerabilities found in the assessment:

- *"<u>Assignment of High-level Information Security Responsibility:</u> Information security is primarily a management function that requires the sustained commitment and attention of high-level officials...A senior management official should be assigned overall responsibility for ensuring that the City takes an enterprise-wide strategic view of its information security program...*
- *<u>Focus on Fixing Most Pressing Security Concerns:</u> The City should conduct a comprehensive analysis of the severity of each of the identified findings and risks within this report, and that all critical issues receive timely remediation...*
- *<u>Development of a Security Architecture Model:</u> ...The security architecture should incorporate security policies, standards and technologies. The architecture should adopt a 'restrictive design.' From a security standpoint, that means 'Everything that is not specifically allowed is denied'...*
- *<u>Implementation of Common Security Tools and Methodologies:</u> The City should focus on identifying and implementing common automated security tools, consistent with the City overall security architecture. The use of common security tools can reduce costs and duplication of effort over time. It also helps to ensure a standard level of protection, and the on-going assessment of such protection levels, throughout the City and its departments/divisions..."*

These major information security initiatives and the other corrective actions recommended by Jefferson Wells assume a Citywide oversight authority for the deployment of computer systems which did not exist before the Mayor's recent initiative to improve information technology governance. Information technology and information security go hand-in-hand. Indeed, as mentioned above, security vulnerabilities are often a direct consequence of the specific technologies deployed. Therefore, it was considered important for this report to include and recognize the new initiative and the implementing ordinances as the organizational basis for the recommendations to improve information security.

Although City information technology management and information security would benefit from greater centralized oversight, the pendulum should not swing back to excessive central control that may stifle creativity and impede the ability of departments to adapt to changing needs. A proper balance should be achieved between the benefits of a standardized network infrastructure that is uniformly secured, and user department control over the computer applications needed to accomplish City business.

Recommendation 1: Implement Most Urgent Risk Assessment Recommendations in 2005

The Chief Information Officer in the Department of Administration should develop an Information Security Improvement Plan to correct the most urgent vulnerabilities identified in the Jefferson Wells Security Risk Assessment Report. The Plan should focus first on those actions that can be accomplished in 2005 without the need for major reorganization or additional funds beyond those available for the 2005 budget. The CIO should report progress to the Mayor and Common Council quarterly.

A top priority should be to harden City networks against external attack by securing all Internet connections, properly managing firewalls and password access controls, implementing a standard Citywide anti-virus solution, and updating network software with the latest security patches, as discussed further in the Jefferson Wells Report.

Recommendation 2: Centralize Information Security

The Jefferson Wells Security Risk Assessment Report indicates that the current decentralized approach to City information security has not been effective in reducing risks. Since information security is integrally related to the actual technologies deployed, responsibility for information technology and security should be assigned together, that is, within a single organization unit. Consistent with the new ordinances, the Department of Administration should have overall responsibility for information security.

The Mayor and Common Council should provide the Department of Administration with sufficient staff and other resources to implement and maintain an effective Citywide information security function.

Recommendation 3: Create Information Security Officer Function

The Jefferson Wells Security Risk Assessment Report states that *"A senior management official should be assigned overall responsibility...A number of [non-City of Milwaukee] organizations are creating new departments that focus solely on information security and privacy issues. A CSO or Chief Security Officer typically heads these departments...The CSO also focuses on the business of information security, allowing the City Chief Information Officer (CIO) and chief technology leaders within departments to focus on the business of IT."*

The Mayor and Common Council should consider creating a new Information Security Officer position in the Department of Administration to coordinate City information security. This position could be created either by restructuring an existing City position or by establishing a new additional position. As this function evolves and proves its value, added staff support may be required.

Recommendation 4: Fully Implement Risk Assessment Recommendations

The new Information Security Officer should coordinate implementation of the remaining recommendations of the Jefferson Wells Security Risk Assessment Report. These recommendations need to be reviewed and carefully considered for action as soon as possible, using a risk-based prioritization. Some actions will require no additional budget resources, such as having all network users sign a security policy document. Most of the departments reviewed had not employed this control. Other actions will require an investment of both time and funds, such as conducting regular vulnerability assessments to identify specific information security risks, their relative importance, and actions to address each risk.

While there may be insufficient time in 2005 to completely quantify and fund information security enhancements for 2006, the highest priority actions among those recommendations awaiting implementation should be included in the 2006 budget request.

City of Milwaukee
2004 Information Technology Funding

Exhibit 1

Direct Funding in 2004 Adopted Budget*

Source: Department of Administration - Budget & Management Division

Department	Salaries[1]	Fringe[2]	Information Technology Services[3]	Equipment[4]	Special Funds[5]	SPAs[6]	Capital[7]	Grant[8]	TOTAL
DOA[9]	$44,396	$16,426	$15,775	$3,000	$0	$0	$0	$795,000	$874,597
ITMD	$2,240,522	$828,993	$683,260	$10,000	$930,000	$50,000	$630,000	$250,000	$5,622,775
Assessor	$154,345	$57,108	$16,500	$0	$45,000	$0	$0	$0	$272,953
Attorney	$0	$0	$77,000	$0	$0	$0	$0	$0	$77,000
DCD	$435,964	$161,307	$35,920	$0	$0	$0	$0	$0	$633,191
Council-Clerk	$125,847	$46,563	$58,000	$15,900	$66,000	$0	$0	$0	$312,311
Comptroller	$347,042	$128,406	$90,000	$43,000	$0	$0	$0	$0	$608,448
Election Commission	$0	$0	$11,350	$0	$0	$0	$0	$0	$11,350
DER	$95,434	$35,311	$9,500	$10,000	$0	$0	$0	$0	$150,245
Fire[9]	$389,020	$120,596	$76,451	$20,000	$85,000	$0	$0	$2,000,000	$2,691,067
Health	$197,290	$72,997	$62,550	$0	$55,000	$0	$0	$50,000	$437,837
Library	$482,160	$178,399	$307,473	$156,243	$0	$0	$0	$799,431	$1,923,707
Mayor's Office	$0	$0	$2,000	$0	$0	$0	$0	$0	$2,000
Municipal Court	$129,148	$47,785	$155,000	$0	$45,000	$0	$250,000	$0	$626,933
DNS	$178,167	$65,922	$73,668	$90,000	$0	$0	$0	$0	$407,757
Police[9]	$1,344,947	$403,484	$684,955	$41,000	$0	$0	$5,000,000	$5,100,000	$12,574,386
Port	$0	$0	$5,000	$0	$0	$0	$0	$0	$5,000
DPW-Admin	$660,968	$244,558	$536,000	$51,000	$0	$0	$626,000	$0	$2,118,526
DPW-Infrastructure	$109,680	$40,582	$78,400	$35,500	$0	$0	$0	$0	$264,162
DPW-Operations	$46,352	$17,150	$92,000	$84,625	$0	$0	$0	$0	$240,127
Treasurer	$97,139	$35,941	$20,980	$0	$69,935	$0	$0	$0	$223,995
ERS	$378,061	$139,883	$120,000	$50,000	$4,500,000	$0	$0	$0	$5,187,944
PABF	$0	$0	$1,000	$2,000	$0	$0	$0	$0	$3,000
Deferred Comp	$0	$0	$2,000	$0	$0	$0	$0	$0	$2,000
Parking Fund	$0	$0	$3,500	$2,000	$0	$0	$0	$0	$5,500
Water Works	$418,452	$154,827	$3,803,500	$409,125	$0	$0	$0	$0	$4,785,904
Sewer Maint. Fund	$0	$0	$50,000	$24,900	$0	$0	$0	$0	$74,900
TOTAL CITY	**$7,874,934**	**$2,796,238**	**$7,071,782**	**$1,048,293**	**$5,795,935**	**$50,000**	**$6,506,000**	**$8,994,431**	**$40,137,613**
Percent of Total	**19.6%**	**7.0%**	**17.6%**	**2.6%**	**14.4%**	**0.1%**	**16.2%**	**22.4%**	**100.0%**

* Direct budgeted expenses for information technology were identified in the 2004 adopted budget using the BMD-2 forms. Direct expenses are explained in the notes below. In brief, by "direct" is meant that the account clearly identifies the expense as related to information technology. There may be additional funds, either directly or indirectly related to information technology, budgeted within other accounts or for other positions that do not clearly identify the funding as information technology related.

Notes:

[1] Salaries are taken from the 2004 adopted BMD-2 forms for the IT positions identified in the "IT positions" worksheet

[2] Fringe benefits are calculated using the fringe benefit rates established by the Comptroller's Office for the 2004 budget

[3] The Information Technology Services subaccount (634500) within the Operating Expenditures (6300) account identifies funding for systems development, systems support, data processing, and IT infrastructure.

[4] The Equipment account (6800) in the BMD-2 identifies new or replacement equipment for computers and accessories, including monitors, peripherals, workstations, software, and printing equipment

[5] Special Funds that were for IT purposes, such as computer replacement, were included

[6] Special Purpose Accounts (SPAs) for IT purposes, such as e-government, were included

[7] Capital projects that focused on IT, such as information systems upgrades or replacement, were included

[8] Grants that involved a significant information technology component, as identified in the BMD-28 form and the Community Development Block Grant allocations, were included

[9] A total of $4,895,000 in grant funding from the Urban Areas Security Initiative Program Grant is included. While this funding was not anticipated when the 2004 budget was adopted, the grant award was received in the 2004 fiscal year subsequent to budget adoption.

Exhibit 2

City of Milwaukee
Security Risk Assessment Report
by Jefferson Wells International

	JWI			Departments	
#	Page	Security Layer	Security Control Item	Out of 9	Security Deficiency
1	14	1 - Policy & Procedure Governance	Citywide Information Security Policy and Standards	4	Did not know about the 1996 City of Milwaukee Information Security Policy and Standards document
				6	Did not follow the 1996 policy document
2	15	1	Risk and Vulnerability Assessments	7	Did not perform some level of risk and vulnerability assessment on a regular basis
3	15	1	Change Control	6	Did not have some level of documented change control policy or procedure
4	16	1	Business Recovery Planning	Half	Did not have documented business recovery plans
5	17	1	Hardware and Software Standardization	9	Did not benefit from Citywide standards for hardware and software
6	18	1	Help Desk Support	Most	Did not utilize the Citywide Help Desk for support
				Most	Did not have documented department policies and procedures for Help Desk support
7	19	2 - Facility	Physical Access Control Procedures	7	Did not have documented access controls for department network equipment and data centers
8	20	2	Emergency Shutdown Procedures	6	Did not have some level of documented emergency shutdown procedures
				9	Did not routinely test emergency shutdown procedures
9	21	3 - External Network	External Firewall	Several	Did not have adequately controlled Internet connections
10	22	3	Firewall Logs	Some	Did not actively review and retain firewall logs
11	22	3	Dial-up Access	9	Did not inventory modem receptive devises on analog phone lines
12	22	3	Change Management	Half	Did not use firewall change control procedures
13	22	3	Firewall Assessments	6	Did not have a policy to review firewall rules on at least an annual basis
14	23	3	Perimeter Router Access Control Lists (ACLs)	1	Did not have an administrative password configured within a router
15	23	3	Separate Internal/External Domain Name Service (DNS) Servers	Most	Did not have separate internal and external DNS systems
16	23	3	DMZ Infrastructure	Several	Did not have DMZ infrastructure surrounding web servers located within the core internal network
17	23	3	System Hardening	4	Did not have policies, procedures or standards for hardening systems
18	24	3	Remote Access Solutions	5	Did not have adequately documented remote access solutions
19	24	3	Security Logon Banners	9	Did not have security logon banners
20	24	3	Intrusion Detection System (IDS)	8	Did not have IDS
21	26	4 - Internal Network	Internal Firewall	6	Did not have internal firewalls to control access to/from other departments
22	26	4	Anti-Virus Solution	1	Did not have a formal anti-virus solution
23	27	4	Patch Management	9	Did not have documented patch management policies and procedures
24	27	4	Printer Security	9	Did not have network printers secured with usernames and passwords
25	27	4	Email Access	Several	Did not use the same email systems
26	28	5 - Platforms	Password Policies	Some	Did not have adequate password protection for network equipment
				Half	Did not regularly change administrative passwords
				Half	Did not have separate user and administrative accounts for administrators
27	29	5	Event Logging and Review Procedures	Half	Did not review event logs on a consistent basis
28	30	6 - Workstations	Password Protected Screensavers	Half	Did not enforce screensaver passwords
29	31	6	Policies and Controls on Removable Media and PDA Devices	7	Did not control the use of removable media such as CD-ROMs
				6	Did not control the use of PDAs
30	31	6	Workstation Re-use Policies and Procedures	Half	Did not have a process for re-deploying workstations
				7	Did not have a documented process for re-deployment
31	32	7 - Databases	Database Audits and Assessments	Most	Did not perform periodic database audits and vulnerability assessments
32	33	8 - Data	Data Classification	Half	Did not classify data and data security roles
				3 qtrs	Did not have policies restricting data transmittal based on data classification levels
33	35	9 - Applications	Application Criticality Analysis	Half	Did not perform an application criticality analysis
34	36	9	Software Inventories and License Audits	Half	Did not inventory software and audit software licenses
35	36	9	Web Server Audits and Application Development Lifecycle	5	Did not have documented application development lifecycle procedures
36	37	10 - People	Security Policy and Awareness Training	7	Did not have all users sign a security policy
				8	Did not provide user security awareness training
37	38	10	Vendor Management	Some	Did not have policies and procedures to manage vendor access

JEFFERSONWELLS INTERNATIONAL

City of Milwaukee

Security Risk Assessment Report

AUGUST 6, 2004

JEFFERSON WELLS INTERNATIONAL
330 EAST KILBOURN AVENUE, SUITE 1075
MILWAUKEE, WI USA
(414) 347-2345

RESTRICTED CONFIDENTIAL

JEFFERSONWELLS
INTERNATIONAL

330 EAST KILBOURN AVENUE, SUITE 1075
MILWAUKEE, WISCONSIN 53202
PHONE 414.347.2345 FAX 414.347.1206
WWW.JEFFERSONWELLS.COM

August 6, 2004

Mr. W. Martin Morics
City Comptroller
City of Milwaukee
200 East Wells, Room 404
Milwaukee, WI 53202

Dear Mr. Morics:

At the direction of the City of Milwaukee ("City"), an Information Protection Architecture Risk Assessment ("IPARA") was performed during the months of December 2003 through June 2004. During the engagement, Jefferson Wells collected documentation and performed interviews with eleven predetermined City departments/divisions. Following the interviews, Jefferson Wells conducted high-level automated network discovery scans on the eleven departments/divisions.

The attached report summarizes the results of this engagement. This report is intended solely for the use of the City of Milwaukee. Jefferson Wells does not take any responsibility for the reliance on this information by any external third parties.

We sincerely appreciated the courtesy, cooperation, and assistance extended to us by the employees of the City of Milwaukee during this engagement. If you have any questions, please contact me at (414) 347-2345.

Sincerely,

Paul R. Rozek

Paul R. Rozek
Director, Technology Risk Management Services

TABLE OF CONTENTS

This report is intended solely for the use of the City of Milwaukee. Jefferson Wells does not take any responsibility for the reliance on this information by any external third parties.

Executive Summary

Engagement Scope and Acknowledgements

The City of Milwaukee ("City") Internal Audit function partnered with Jefferson Wells International, a professional services firm based in Milwaukee WI, to perform a high-level risk assessment. This assessment focused on the City information security practices and processes used to help ensure the confidentiality, integrity, and availability of the City information assets.

This Security Risk Assessment Report reflects the results of the Jefferson Wells engagement conducted over the time period of December 2003 – May 2004. Employed information-gathering techniques included interviews, observations, documentation reviews, and use of third-party vendor technical security scanning software products.

Jefferson Wells personnel, working under the direction of the City Audit Supervisor, assessed security risks in the following alphabetical list of eleven City departments/divisions (the list was provided to Jefferson Wells to include within the scope of this assessment – in other words, the eighteen other City departments/divisions were not assessed):

- City Clerk / Common Council
- Department of Administration (ITMD)
- Department of City Development (DCD)
- Department of Public Works (DPW)
- Employees' Retirement System (ERS)
- Milwaukee Fire Department
- Health Department
- Milwaukee Public Library
- Municipal Court
- Milwaukee Police Department
- Water Works (DPW)

During the course of this risk assessment, the Milwaukee Police Department provided no information, no interviews, and no opportunities for scanning its networks and servers for security risks. The Milwaukee Fire Department provided limited documentation and no interviews (however, scanning of its networks and servers were allowed).

At no time did Jefferson Wells attempt to exploit any of the security risks and vulnerabilities identified during this assessment. It should be noted that no series of process assessments and technical scans could uncover all potential security risks to an organization such as the City of Milwaukee. Additionally, our risk assessment activities were conducted within a finite timeframe, budget, and scope. Accordingly, Jefferson Wells cannot guarantee the City computing environment against unauthorized access or activities. Risk assessments are only one part of a comprehensive security and control program. The findings and associated recommendations are provided to support City leadership efforts to reduce overall IT risks and to employ secured, controlled and functional data processing services.

Jefferson Wells wishes to extend its thanks to City personnel for their support and assistance throughout this assessment. The skills, knowledge, and cooperative spirit displayed by all levels of City department/division IT staff contributed to both the completeness and accuracy of this report.

High-level Overview of City Security State

Going back to 2003 and prior, representatives from both the Internal Audit Department (Mr. Jim Michalski) and the Information Technology Management Division (ITMD – Mr. Randy Gschwind) had formally expressed concerns with an apparent lack of coordinated and enforced policies, procedures, and controls that help to protect the City networks and systems. The City has a decentralized information technology architecture with many different types of hardware and software, interfaces, and exposures to outside agencies and facilities – most of these not under the "umbrella" of the ITMD security infrastructure. The Milwaukee Information Policy Committee ("MIPC") has been formed to help promote citywide control initiatives and consists of members from the Mayor's office, the City Comptroller and Treasurer's offices, and the Common Council.

While the ITMD security infrastructure is meant to protect the ITMD and shared resources portions of the City information technology infrastructure, in reality, the City IT network is an interconnection of departmentally managed security programs and solutions. The overall security of the City information assets is truly only as strong as its weakest link. Accordingly, all City departments and divisions must be examined for security risks and then audited to ensure the approved security controls are effectively working as designed over time.

The security risk assessment identified that the City has a process and technical security controls that range from "positive" to "inadequate." Highlights of the risks associated with such controls are provided within this detailed "layers" sections of this report.

Based upon responses in interviews and documentation obtained through questionnaires, several of the departments/divisions appeared to have reasonable security controls and had formal department/division level security policies and procedures. It was observed that City department/division managers and their respective IT representatives were generally aware of the implications of the control questionnaires and security comments discussed by Jefferson Wells personnel and, that City personnel demonstrated an interest to maintain and/or strengthen their current security controls. However, Jefferson Wells is unable to comment on the ongoing effectiveness of the observed controls at this time because a detailed and comprehensive audit of security policies and related process and technical controls were outside of the scope of this engagement.

This report is intended solely for the use of the City of Milwaukee. Jefferson Wells does not take any responsibility for the reliance on this information by any external third parties.

The following items are examples of identified security risks that are further discussed within this report:

- Lack of planning related to centralized/decentralized security programs and lack of governance over security initiatives and controls
- Lack of current security self-assessments and awareness efforts
- Lack of enforcement of security policies, procedures, and solutions used with managing access to City information assets
- Lack of enforced standards for technical configurations and business processes that reduce and/or prevent security risks
- Inadequate citywide monitoring programs in place to detect security risks and report weaknesses
- Lack of centralized solutions to track and resolve potential security risks and/or problems on a timely basis

The overall state of risk the City faces in regards to information security is considered serious. While some departments/divisions within themselves have controls in place to reduce risks to their own segments of the network, the decentralization and lack of citywide governing controls will continue to hinder the City from creating a secure, interconnected environment. We highly recommended that the City evaluate the effectiveness of the current decentralized network environment and consider addressing information security controls on a timely basis from a centralized, citywide, point of view.

To enhance the overall Information Security program for the City, Jefferson Wells recommends pursuit of the following four high-level initiatives. (Relevant root-causes and potential costs for the implementation for each of these initiatives were not readily ascertained during this risk assessment engagement.)

1. <u>Assignment of High-level Information Security Responsibility</u>

   Information security is primarily a management function that requires the sustained commitment and attention of high-level officials at the City and department/division levels. To this end, we strongly believe that the current individual departments' IT security functions should be elevated and strengthened. A senior management official should be assigned overall responsibility for ensuring that the City takes an enterprise-wide strategic view of its information security program.

   Ownership of this security decision-making process is critical to its long-term success. A number of organizations are creating new departments that focus solely on information security and privacy issues. A CSO or Chief Security Officer typically heads these departments. The CSO is assigned to relieve the City departments of the need to manage strategic planning for security and privacy issues and, assist City leadership in the budgeting process by creating a clear demarcation for security-related expenses. The CSO also focuses on the business of information security, allowing the City Chief Information Officer (CIO) and chief information technology leaders within departments to focus on the business of IT.

This report is intended solely for the use of the City of Milwaukee. Jefferson Wells does not take any responsibility for the reliance on this information by any external third parties.

The CSO should develop and implement a coordinated and effective IT security program that is continuous, iterative, and fully integrated with IT architectures and City services. The CSO's role should involve seven major activities:

1. Planning to ascertain threats and risks within all City departments/divisions
2. Assessing the current levels of protection and their effectiveness
3. Collaborating with City executives, MIPC, ITMD, and other IT security liaisons
4. Managing the Security Architecture Model (described on the following pages)
5. Integrating enterprise security controls and solutions within the City
6. Responding to security incidents and determining fixes to "root-causes"
7. Enforcing "penalties" for non-compliance with approved security controls.

To be effective, this role requires support of City executives and requires the authority, responsibility, and accountability to implement and enforce security policies and procedures and to penalize departments/divisions that are not in compliance.

2. Focus on Fixing Most Pressing Identified Security Concerns

The City should conduct a comprehensive analysis of the severity of each of the identified security findings and risks within this report, and that all critical issues receive timely remediation. (Note: this is an on-going activity of a CSO.) The City should also develop a centralized database for tracking the remediation of security weaknesses. This database should be a common repository of findings and corrective actions identified through IT self-assessments and/or independent verification and validation activities (e.g., audits by Internal Audit).

Over time, the City should use this database to help prioritize and monitor the implementation of corrective actions. It should increase monitoring of compliance with departmental policy and help ensure that costs for security are identified in IT budgets and strategic plans. At the same time, information within the database should supply support for individual departments/divisions and/or citywide solutions for interdepartmental problems. For example, one department/division may be implementing a common web-based security education and awareness program that should be available to all City departments.

3. Development of a Security Architecture Model

It was identified that City departments were evaluating various technology solutions to improve the security of its systems. However, there was no overall citywide approach or architecture to guide these efforts. For example, many of the City network devices are running older and less secure versions of operating code. As a result, enterprise security solutions might not be able to be implemented due to isolated and "patchwork" security defenses.

The City should develop an Information Security Architecture, employing a "Defense-in-Depth" model, consistent and integrated with the City enterprise IT architecture. The security architecture should incorporate security policies, standards and technologies. The architecture should adopt a *"restrictive design."* From a security

This report is intended solely for the use of the City of Milwaukee. Jefferson Wells does not take any responsibility for the reliance on this information by any external third parties.

standpoint, that means *'Everything that is not specifically allowed is denied.'* If combined with adequate logging and monitoring, any attempt to make use of the City network in an unauthorized manner will probably fail and it should be noticed in a timely manner.

A security architecture will enable a department/division to better identify its security risks and possible solutions, and, help to eliminate implementation of inconsistent security approaches. The security architecture and policies will continually evolve in support of the security process. The process itself should contribute to the future City systems' growth and change, and, the continual analyses of the security architecture and policies will suggest future enhancements/changes to the security process.

The architecture should be subject to regular and comprehensive audits. Audits evaluate the effectiveness of controls through the use of formal methodologies and testing activities. A network security audit provides a metric by which the quality of the security program can be judged by City executives.

Two common types of audits are penetration studies and configuration analyses. A penetration study is a type of audit in which the auditor approximates what an attacker would do, such as scanning machines for network services, determining the versions of those services, and applying exploitation techniques to gain access to the network. Limitations placed on the auditor may impact or bias the results away from what an actual attacker (with no constraints) might be able to achieve. A configuration analysis audit is used to examine the network from the inside using a highly detailed work program. This type of audit is typically more thorough than penetration studies, is easier to schedule than a penetration study, and can be performed with less impact on production systems. This type of audit requires a highly skilled auditor – not just a tool operator – and requires extensive analysis and correlation of data to identify potential security risks and exposures.

4. Implementation of Common Security Tools and Methodologies

Today's emerging security technology enables a level of protection that only a few years ago was either not achievable or not cost-effective. For example, network based authentication and auditing tools are now able to prevent and detect the majority of unauthorized system access and use. Virtual Private Network (VPN) technologies improve boundary protection by funneling network traffic through strong, professionally managed gateways.

The City should focus on identifying and implementing common automated security tools, consistent with the City overall security architecture. The use of common security tools can reduce costs and duplication of effort over time. It also helps to ensure a standard level of protection, and the on-going assessment of such protection levels, throughout the City and its departments/divisions.

The City is specifically encouraged to consider timely acquisition and implementation of technical security scanning software to facilitate its own regular self-assessments

This report is intended solely for the use of the City of Milwaukee. Jefferson Wells does not take any responsibility for the reliance on this information by any external third parties.

of IT security risks over its external and internal networks, servers, workstations, and databases. In addition, centralized monitoring solutions that consolidate and correlate security event data across multiple servers should be considered.

This report is intended solely for the use of the City of Milwaukee. Jefferson Wells does not take any responsibility for the reliance on this information by any external third parties.

Considerations Related to "Reengineering" Security at the City

E-Government and other strategic initiatives

The following are information technology changes, provided by the City, which are either "in process" or "planned" to create efficient, economical, and secure electronic (e-commerce) business processes. In general, these following initiatives are used to promote enhanced "open communications" – in areas such as Government-to-Government (G2G), Government-to-Business (G2B), and Government-to-Citizen (G2C):

- E-mail (internal: calendar, City business; external: City vendor quotations, agreements, e-notify - notification of services offered by Milwaukee.gov)
- E-payments with credit / debt cards (Treasurer taxes, License Division licenses, Record Center copies, DPW parking permit and citations, Municipal Court fines, City ProCard purchases),
- E-fund management (Employee Retirement System planning)
- E-employee maintenance (Comptroller employee data for accounting and payroll)
- E-public query (Assessor property data, Common Council legal code, Treasurer taxes, Deferred Compensation planning, DPW bids and service requests, Election results, ERS pension calculations, Health Dept services, Library services, MPD services, Purchasing bids, Property assessment)
- Wireless Voice and Video-over-Internet Protocol devices (Police and Fire radio systems; City phone system; secure network access for City Managers: laptops, work-stations, printers, PDAs, video-cell-phones; Common Council meeting video broadcasts)

Additional "openness" inherently creates the potential for increased security risks. Deployment of these initiatives requires effective security analyses and consistent security management involvement during the planning, development, testing, integration, and acceptance phases of each project.

Milwaukee Information Policy Committee

The Milwaukee Information Policy Committee ("MIPC") was formed and consists of members from the Mayor's office, the City Comptroller and Treasurer's offices, and the Common Council. The duties of the MIPC, as defined in the Milwaukee Code of Ordinances, included:

- Recommending policies to the Mayor and the Common Council for the management of the City electronic information resources, including but not limited to access, distribution, documentation, security and appropriate use.
- Promoting interdepartmental and intergovernmental sharing of electronic information resources.
- Promoting the use of electronic information resources to improve the policy-making process and administration of City government.

- Promoting public access to the City electronic information resources.

Security policies affect everyone, and in theory, everyone should have some say in the policies. The MIPC membership should possess a cross-section of relevant skills and backgrounds, and have the authority from City executives to create and enforce policies. Without strict policy enforcement, challenges to security policies, such as a result of an involuntary employee termination, might not hold up in court.

In the future, we also recommend that the MIPC serve as an advisory group for future strategic security initiatives and help the CSO gauge the level of security awareness and competency across the City.

This report is intended solely for the use of the City of Milwaukee. Jefferson Wells does not take any responsibility for the reliance on this information by any external third parties.

"Defense-In-Depth" Model

Overview of the Defense-In-Depth Model

In the information age in which we live, more and more individuals, businesses, corporations, local/state governments, and countries are becoming interconnected through both wide-area and global networks (such as the Internet). Information to the public is "on demand" practically anytime and anywhere. The lifeblood of a global economy depends on the networks being available – for example, it's hard to imagine day-to-day life without email.

The ideas of *always connected*, *instant information*, and *data sharing,* while remaining productive and efficient, come with substantial risks. As a result, Information Security professionals are required to focus attention on minimizing risk while maintaining the three internationally-recognized principles of information security: *Confidentiality, Integrity*, and *Availability*. In order to accomplish these principles, many organizations are embracing the design, implementation, and regular maintenance of a strategy known as the **Defense-in-Depth.**

The concept of Defense-in-Depth is to use multiple defense mechanisms or layers across your network infrastructure to protect internal data, systems, networks, databases, and people. Why do security experts place such a premium on layering? The reason is brutally simple:

> *There is* ***no*** *single defense, system, method or design that is proof against all forms of attack/intrusion.*

If there were, of course, then network security would be easy — everyone would use whatever that was! Since this doesn't exist, we are automatically forced to consider *effective combinations of approaches* when designing security controls.

The following ten sections of this report are structured to provide insights on the ten layers within the Defense-in-Depth model that applies to the City. Each layer will be identified, and then highlighted with a description and/or best practice related to the business processes and/or technology employed by City departments. In addition, risks associated with each layer will be generalized, i.e., specifically not to identify the department(s) exhibiting the stated risk(s).

It is critical to acknowledge that there is no correlation to the numbering of the security layers presented in this report – the number of the layer does not designate its priority level. In the future, City management (i.e., the future CSO and the MIPC) will have full discretion as to which layer(s) to address and in what priority. It should be noted that the layers are "interdependent" – meaning that a weakness in one layer may directly increase the risk(s) of other layer(s) being compromised.

This report is intended solely for the use of the City of Milwaukee. Jefferson Wells does not take any responsibility for the reliance on this information by any external third parties.

As a result of this risk assessment, Jefferson Wells believes the City should first address the risks identified on the external perimeter of the network, such as web servers, firewalls, and external routers. Once the external perimeter of the network is hardened and audited, further audits and assessments should be performed on internal network controls.

There may be times throughout our assessment process, or within this report, when specific types of hardware, software, or services may be mentioned as potential security and control solutions for the City. Jefferson Wells International does not do this as an endorsement of any kind. The implementation of any security solution(s) must be carefully evaluated for relevance to current City IT needs, risks, budgets, and personnel, and, the current and future products and services offered to the citizens of the City of Milwaukee.

This report is intended solely for the use of the City of Milwaukee. Jefferson Wells does not take any responsibility for the reliance on this information by any external third parties.

Security Layer #1 – Policy & Procedure Governance

Overview and General Observations

Security begins with the culture and tone sent down from senior management and the Common Council to city departments and employees. This culture and tone is defined through policies and procedures. Policies help to define the information assets the City considers valuable. Policies also help to identify the City's security goals and objectives. Equally important, policies facilitate personal responsibility and accountability and give authority to the security activities. Procedures are used to further define the processes to be followed to implement the security controls described in the policies.

During the assessment, the following general observations were noted:

- Citywide policies and procedures awareness is limited and lack enforcement.
- In general, City departments are operating on their own standards and practices, which are not formally defined and documented.
- The lack of standardization of hardware, software, and support services utilized throughout City departments further impairs the City efforts to develop a cohesive infrastructure with effective interdepartmental communications.

Areas for Security Controls Enhancement

During the assessment, the following areas for controls enhancement were identified:

Control Item – Citywide Information Security Policy and Standards:
The current City of Milwaukee Information Security Policy and Standards document dates back to 1996. Based on the interviews conducted with nine city departments, only five acknowledged the existence of this document. Of these five, two stated they follow the policy and one stated they partially follow it. Common critiques of the policy were that it was outdated and lacked an enforcement authority.

Beyond policies and procedures defined at a citywide level, three of the departments acknowledged having some level of departmental policy and procedures in place. For most of the departments not having such documents, the reasoning behind not having them was mostly due to not having the time or resources available for developing and implementing polices and procedures.

Recommendations:
Without awareness and an enforcement authority, a policy can be looked as no more than a document. This policy, as well as other policies and procedures, must be periodically (i.e., at least annually) reviewed and updated to ensure they are still relevant to changing technology and citywide business needs. All employees affected by the policy need to be informed and acknowledge these documents, including periodic reminders. Policies must have defined sanctions, making it clear to all what the potential results are for noncompliance.

This report is intended solely for the use of the City of Milwaukee. Jefferson Wells does not take any responsibility for the reliance on this information by any external third parties.

An enforcement authority must be clearly present and actively monitor city activities and initiatives, to ensure they align with citywide goals. This enforcement generally comes from the Chief Security Officer ("CSO") role, as defined and recommended earlier in this report under the Key Engagement Action Items. The CSO should engage department/division heads and representatives in the development and maintenance of security policies and procedures.

While it may not be necessary for all departments to have individual security policies and procedures, the need for such documents should be reviewed. Departmental policies and procedures should be developed and maintained for departments with additional security needs not covered in a citywide policy. It is important that any departmental policies and procedures developed are not in conflict with policies and procedures at the citywide level.

<u>Control Item – Risk and Vulnerability Assessments:</u>

Of the nine departments interviewed, only two of the departments stated that they perform some level of risk and vulnerability assessments on a regular basis. Other department comments included not performing any assessments or running system-scanning tools on a sporadic, "as needed", basis.

Recommendations:

Risk assessments and vulnerability assessments should be an integral part of the security program for each city department/division. These assessments should be performed on a regular and formal schedule determined by the level of risk associated with each department/division, but no less frequently than on an annual basis.

The initial assessments should be performed and used as a baseline for future assessments. Action items should be documented for follow-up and resolution, based on the risks determined. Periodic assessments are necessary because of changing technology and vulnerabilities in the City.

The need and requirements for these security risk and vulnerability assessments should be defined within the citywide Information Security Policies and Procedures. The responsibility for performance of the assessments should fall on City department/division leaders. The department/division leaders should in turn work closely with the CSO role. Since the departments/divisions within the City are interconnected via the network backbone and shared systems, risks defined within one department/division may cause additional risks for other departments/divisions.

<u>Control Item – Change Control:</u>

Change control is defined as the process of planning, documenting, communicating, and executing changes to hardware or software in the City infrastructure. Three of nine departments/divisions interviewed stated they have some level of documented policy and/or procedure relating to change control. It was noted that a citywide change control policy was composed, approved, and rolled out circa 1994, however it was never formally adopted or enforced.

This report is intended solely for the use of the City of Milwaukee. Jefferson Wells does not take any responsibility for the reliance on this information by any external third parties.

Recommendations:

The City of Milwaukee should evaluate the current citywide change control policy, update it as necessary, and roll it out to all departments/divisions. This policy should be detailed enough to have meaning, but open enough to accommodate the individual needs of the various city departments/divisions. Departments/divisions, within themselves, should in turn develop more specific change control procedures for the various systems in place. As mentioned earlier, policies define goals and objectives, while the procedures define the processes to be followed, or the "how to."

To ensure citywide systems are maintained to a standard defined level of security, the City should develop formal standards and baselines for applications and platforms that all departments/divisions must follow. These standards and baselines should define minimum lockdown procedures and controls that must be in place for the application or platform. This process of implementing such standards is typically referred to as "security hardening." When such changes are implemented, the application or platform should be tested or "certified" to ensure new security controls are effective and, that the changes did not adversely impact any existing security controls.

There are different industry methods for developing change control policies and procedures. An effective change control policy and procedure should include the following:

- Formal documentation of current configurations
- A change control request and approval process
- A documented test plan with back-out procedures
- Implementation
- Post-installation testing procedures
- Application / platform certification
- Change information and training for end users and support staff
- Vendor support documentation
- A change control tracking mechanism

A common misconception of many organizations regarding change control is that it is an IT function. In reality, it is a process that involves the entire department/division and possibly the city as a whole. It is critical to define roles and responsibilities within this process to ensure all end users and department/division managers affected by a change are involved in the process from the beginning.

Additional observations and recommendations regarding change control will be addressed in other Defense-in-Depth layers in this report.

<u>Control Item – Business Recovery Planning:</u>

Based on the nine departments/divisions interviewed, about half stated that they have documented business recovery plans, either complete or partial. The majority of these are considered in need of updating or not being formally tested. The City Information Security Policies and Standards document states a requirement that each department/division shall establish procedures for contingency planning and disaster

This report is intended solely for the use of the City of Milwaukee. Jefferson Wells does not take any responsibility for the reliance on this information by any external third parties.

recovery. It also states that validation and periodic reevaluation of the practices and procedures are performed.

Recommendations:
Business recovery plans should be required for all City departments/divisions housing a data center with business critical information. Since many of the departments/divisions within the City are interconnected, coordination between departments/divisions sharing information systems is critical. Guidelines and requirements of departmental business recovery plans should be further defined in the City Information Security Policies and Standards. Updating and testing of these practices and procedures is necessary to help reduce the loss of services in the event of an emergency. The City departments/divisions should be responsible for the development and coordination of services with other departments/divisions as necessary. The CSO role should be assigned with the responsibility of ensuring all departments/divisions are following the stated policies and guidelines established.

Control Item – Hardware and Software Standardization:
It was observed that departments/divisions citywide were able to independently define and acquire the types of hardware and software to use – including workstations, network equipment, firewalls, and application products. Most of the departments/divisions interviewed stated that they do follow some level of standardization within their department/division, but few had the policy documented. No citywide policies or standards were noted during the assessment.

Recommendations:
The City should review the citywide purchasing of software and hardware to determine the most beneficial method of standardization. Citywide standardization can benefit the City in many ways, including:

- Reduced costs due to volume discounts negotiated with a reduced number of vendors.
- Reduced costs for maintenance and support contracts for hardware and software.
- More efficient use of centralized internal support staff. While a comprehensive IT infrastructure requirements analysis was not performed, with the current number of non-standard equipment, network platforms, and specialized hardware and software, the City probably needs to maintain a larger number of specialized support staff to maintain its systems.
- Standardization of hardware and applications will reduce the communications and compatibility conflicts between equipment and applications, allowing for a more cohesive and interconnected network environment.
- Flexibility should be incorporated into the standards to ensure specialized department/division needs are addressed.

This report is intended solely for the use of the City of Milwaukee. Jefferson Wells does not take any responsibility for the reliance on this information by any external third parties.

Control Item – Help Desk Support:

The City has a citywide Help Desk available, however most departments/divisions reported that they provide their own Help Desk services. Only a couple of the departments/divisions were actually performing logging of the calls, while some were in the process of evaluating Help Desk applications. Of the departments/divisions utilizing Help Desk tracking applications, the majority was using Track-IT©. Few of the departments/divisions had formal documented policies or procedures in place regarding Help Desk support.

Recommendations:

The City should evaluate current Help Desk procedures throughout the various departments/divisions. A more centralized and cohesive Help Desk policy should be developed and implemented throughout the City. This policy should formally define what equipment and applications are supported through central IT groups and which should be supported within the departments/divisions themselves. Standards should be developed and implemented requiring logging of support calls with resolutions. Ideally this system would be centrally located, providing a less fragmented approach to call monitoring and logging. The central IT groups should be responsible for support on applications shared across multiple departments/divisions and individual department support staff should be utilized for department/division specific applications and "at-the-desk" support.

Centralization of Help Desk support would reduce the overhead and cost of support staff citywide. Allowing the central support staff to receive and handle the majority of the support calls, department/division support staff will be enabled to address the more pressing tasks of the department/division. Centralized logging can provide the City with systems performance metrics and the ability of monitoring for potential incidents affecting multiple departments/divisions citywide.

Cost savings may also become apparent by combining the various applications and licensing of the tracking and support applications. A properly implemented centralized support application can provide the City with accurate and up-to-date information regarding citywide support calls, license tracking, and software implementations.

This report is intended solely for the use of the City of Milwaukee. Jefferson Wells does not take any responsibility for the reliance on this information by any external third parties.

Security Layer #2 – Facility

Overview and General Observations

The "Facility" layer of security is commonly referred to as the physical security of the environment. This layer includes topics such as physical access to data centers and telecommunications equipment; environmental controls; fire, smoke, and water detection; related alarm notification; auto-fire suppression; and emergency procedures. The physical security and controls of an environment are just as important as any of the other more technical control layers.

It is important to note that physical facility walkthroughs were not performed within the scope of this assessment.

During the assessment, the following general observations were noted:

- The larger data centers within the City infrastructure appeared to have controls regarding physical access.
- Departments/divisions with a smaller amount of network equipment generally had less stringent controls.
- It was noted during most department/division interviews that controls were in place to restrict access to hardware and software manuals, software installation media, and storage of additional hardware.

Areas for Security Controls Enhancement

During the assessment, the following areas for controls enhancement were identified:

Control Item – Physical Access Control Procedures:
Physical access controls to the larger data centers of the City appear to be controlled. Network equipment in the departments/divisions with a smaller amount of equipment were less stringent. Of the nine departments/divisions interviewed, only two of them had partially to fully documented access control procedures to network equipment and data centers. The City Information Security Policies and Standards document states "Each department, division, or agency must provide for the physical security of the information processing infrastructure."

Recommendations:
With the citywide network backbone connecting numerous departments/divisions together, it is extremely important to consistently control the physical security of the information-processing infrastructure from all points of access. With today's technology, it is not as important for an attacker to gain physical access to the "target" data center. In many cases it is more practical for the attacker to gain control and access through another point of access that is interconnected and has less stringent controls in place. In the scenario of a government entity, many of these interconnected

This report is intended solely for the use of the City of Milwaukee. Jefferson Wells does not take any responsibility for the reliance on this information by any external third parties.

departments/divisions receive a large amount of public traffic, reducing the risk of the attacker being detected.

The City should perform a thorough evaluation of the physical security of the information-processing infrastructure for all departments/divisions. A baseline of physical security policies and standards should be developed and implemented in the Information Security Policies and Standards for all departments/divisions. Beyond this baseline for all departments/divisions, each department/division should continue to be responsible for evaluating and implementing, if necessary, additional controls as determined by the individual risks of the department/division.

Control Item – Emergency Shutdown Procedures:

Of the nine departments interviewed, three departments/divisions reported having some level of documented procedures regarding emergency shutdown procedures. None of the departments/divisions reported formal testing of these controls, except for in "real life" scenarios.

Recommendations:

Emergency shutdown procedures should be a requirement defined in the Information Security Policies and Standards document. Each department/division should formally document these procedures and perform shutdown testing on at least an annual basis. The procedures should define the roles and responsibilities of the individuals involved and provide for training these individuals on the tasks to be performed.

Types of emergencies to consider in these procedures should include, but may not be limited to:

- Loss of electricity, heat, air conditioning, water or other essential utilities
- Failure of mechanical equipment such as HVAC systems and emergency generators
- Flooding, tornadoes, or other natural disasters
- Nearby chemical releases of hazardous materials to the environment
- Terrorist actions or civil unrest

This report is intended solely for the use of the City of Milwaukee. Jefferson Wells does not take any responsibility for the reliance on this information by any external third parties.

Security Layer #3 – External Network

Overview and General Observations

The City maintains a large number of hardware and software systems that provide vital information for the City of Milwaukee business processes. The technical vulnerability scans performed by Jefferson Wells provided valuable information and insights into the City of Milwaukee external network security architecture and how that architecture might be vulnerable. However, the scans provided a "snapshot-in-time" description of the external network security state.

During the assessment, the following general observations were noted:

- Several different departments/divisions have independent Internet connections, including one Digital Subscriber Line ("DSL") connection with no firewall.
- External network controls vary greatly by department/division, few have Intrusion Detection Systems ("IDS"), and there were a wide variety of firewall and anti-virus solutions.
- The lack of standardization of hardware, software, and support services utilized throughout City departments/divisions further impairs the City from developing a cohesive externally secure infrastructure with effective interdepartmental communications.

Areas for Security Controls Enhancement

During the assessment, the following areas for controls enhancement were identified:

Control Item – External Firewall:

Several different departments/divisions throughout the City had their own separate Internet connection, with their own separate external security. In one case, a DSL connection was found with no firewall or any kind of external protection.

Additionally most departments/divisions were not aware of additional Internet connections from one department/division to the next, or what if any security was in place on those connections.

The current network configuration exposes the City to risk, as several departments/divisions have their own Internet connection. These additional Internet connections have inadequate controls on them, which fall outside of the control of the rest of the City. Additionally it was observed that other departments/divisions within the City were not aware of these connections, exposing other departments/divisions connected to that department/division to be at risk as well.

Recommendations:

The City should have a limited number of external Internet connections controlled through one central location with one standard set of security measures. In limiting the

This report is intended solely for the use of the City of Milwaukee. Jefferson Wells does not take any responsibility for the reliance on this information by any external third parties.

number of external Internet connections, the City greatly increases its security by having direct knowledge (for all departments/divisions) exactly where people can/cannot enter the City network from the Internet. Additionally, this would provide a cost savings for the City by allowing all departments/divisions to share one or two high-speed Internet connections, as opposed to many lower-speed connections to many different departments/divisions.

Control Item – Firewall Logs:

During the assessment, it was learned that some departments/divisions were actively reviewing and retaining firewall logs, while other departments/divisions were not.

Recommendations:

All departments/divisions should review firewall logs at least weekly and retain logs for a management-defined period of time (e.g., at least one year).

Control Item – Dial-up Access:

It was reported to Jefferson Wells during the assessment that there were numerous (i.e., approximately 1,000) analog phone lines citywide that could potentially be connected to modems, allowing direct access into the City networks and/or systems.

Recommendations:

A formal audit should be conducted to determine the number of potential "listening" devices attached to analog phone lines throughout all departments and divisions. This type of audit is commonly called "war dialing" – where a specialized security application is used to automatically dial all phone numbers within the telephone exchanges assigned to the City. The application scans the exchanges for devices that respond to the call. In many cases, the application can determine the type of device responding. The results from a "war dialing" audit should then be compared to the known inventory of networked devices. Unknown devices should be tracked down and disabled if not required.

Control Item – Change Management:

About half of the departments/divisions interviewed during the risk assessment used change control procedures when making changes to the firewall.

Recommendations:

All City departments/divisions should develop formal firewall change control procedures to track any modification, upgrade, or patch to the firewall.

Control Item – Firewall Assessments:

One third of the departments/divisions interviewed during the risk assessment informed Jefferson Wells that they had in place a process, policy, or procedure to review firewall rules on an annual basis. As new vulnerabilities are discovered, and services added and removed in the "fast-paced changes" of IT, it is important to review firewall rules on at least a quarterly basis. One goal of such reviews is to remove any firewall rules that were setup for business purposes and/or for connections that no longer exist.

This report is intended solely for the use of the City of Milwaukee. Jefferson Wells does not take any responsibility for the reliance on this information by any external third parties.

Recommendations:
All departments/divisions should review, on at least a quarterly basis, each rule used on its firewall(s) for a valid business need and remove any unnecessary rule(s).

Control Item – Perimeter Router Access Control Lists ("ACLs"):
One department had a perimeter router that had no administrative password configured within the router. This configuration occurred because of a lack of standards in configuring network equipment. (Please see the control "System Hardening" for more details.)

Recommendations:
All perimeter router ACLs should be reviewed at least annually. Furthermore, all network routers should be adequately hardened for security before being deployed into production.

Control Item – Separate Internal/External Domain Name Service ("DNS") Servers:
Each department/division utilized a different solution for DNS services. Few departments/divisions included separate internal and external DNS systems. Separating the internal and external DNS reduces the risk of the City DNS entries from unauthorized modification if an attacker took control of the domain.

Recommendations:
The City should utilize an internal/external DNS system whenever possible. Additionally there can be cost savings in centralizing DNS within the City, as this is a service that every department/division in the City must utilize for Internet access, and can be a shared common resource.

Control Item – DMZ Infrastructure:
Several departments/divisions had web servers accessible to the public located directly within the core of the City internal network, with no DMZ infrastructure in place.

Recommendations:
Standards and procedures should be adopted citywide establishing an infrastructure by which all externally accessible machines are placed into a secure DMZ.

Control Item – System Hardening:
Four of the nine departments/divisions assessed did not have any policies, procedures or standards for hardening systems at the time of this risk assessment. Without standard-hardening procedures, there is no baseline security that systems are configured to, which would allow the City to maintain a minimum-level of security.

Recommendations:
All departments/divisions should have procedures in place to harden all systems within their networks. These procedures should establish a minimum-security baseline, installing patches and hotfixes, to bring all systems up to a minimum baseline level of security.

Control Item – Remote Access Solutions:

Five of the nine departments/divisions assessed reported that remote access solutions were inadequately documented.

Recommendations:

All remote access solutions should be documented, reviewed and formally authorized.

Control Items – Security Logon Banners:

None of the departments/divisions assessed had security logon banners on their systems. Having a security logon banner is essential to any network, as without a logon banner, the City can potentially lose the ability to litigate a matter if a system is compromised. Additionally, if there is an internal compromise, prosecution is difficult as the defense of "expectation of privacy" may be used.

Recommendations:

All shared resource computer equipment in the City should have a logon banner enabled that clearly states that use of City systems are for authorized City of Milwaukee business only, that all activity is being monitored, and that use of the system serves as "consent to monitor."

Control Item – Intrusion Detection System ("IDS"):

Only one department in this assessment had any form of IDS. Additionally the one department that had an IDS utilized a shareware-based version with no formal corporate support.

Industry surveys have reported cost savings and reduced recovery time frames within firms using formal incident response programs.

Incident Response ("IR") Program Survey

Costs of Security Incidents			
(Year)	2001	2002	2003
Without IR Program	$113,000	$90,000	$110,000
With IR Program	$25,000	$14,000	$15,000
Mean Days to Recover			
(Year)	2001	2002	2003
Without IR Program	23	20	23
With IR Program	10	4	4

Source: Guardent (www.guardent.com; based on a three-year review of 200 incidents at 175 companies.

Recommendations:

As the City centralizes its Internet access points, IDS should be deployed wherever Internet access allows incoming traffic to the City network. IDS should be centrally managed and controls related to its operation should be formally documented.

Detection of potential incidents is not an effective security solution by itself. The City should develop and implement citywide policies and procedures for incident response. Incident response policies and procedures should include definitions of the types of incidents being detected, the response procedures to be followed, and incident logging/reporting standards.

This report is intended solely for the use of the City of Milwaukee. Jefferson Wells does not take any responsibility for the reliance on this information by any external third parties.

Security Layer #4 – Internal Network

Overview and General Observations

The City maintains a large number of hardware and software systems that provide vital information for the City business processes. The technical vulnerability scans performed by Jefferson Wells provided valuable information and insights into the City internal network security architecture and how that architecture might be vulnerable. However, the scans provided a "snapshot-in-time" description of the internal network security state.

During the assessment, the following general observations were noted:

- Most departments/divisions have different vendors of both hardware and software.
- Most departments/divisions have cross-departmental access to each other's internal network.
- The lack of standardization of hardware, software, and support services utilized throughout City departments/divisions further impairs the City from developing a cohesive internally secure infrastructure with effective interdepartmental communications.

Areas for Security Controls Enhancement

During the assessment, the following areas for controls enhancement were identified:

Control Item – Internal Firewall:

Three of the departments/divisions interviewed during the assessment had internal firewalls in place controlling access to/from their specific department/division to other departments/divisions. Internal firewalls can be used to limit network traffic to authorized data – reducing the risk of one department/division's compromise further compromising multiple departments/divisions.

Recommendations:

The City should deploy centrally managed firewalls at each department/division to control access to/from its resources from other departments/divisions. By securing sections of the network, if one department/division's systems are compromised, that breach may be restricted to just that department/division.

Control Item – Anti-Virus Solution:

Each department/division currently could currently select its own anti-virus solution and at least one department/division did not have any formal anti-virus solution.

Recommendations:

The City should implement a standardized "citywide" anti-virus solution at the workstation, server, and gateway levels. This solution should include centralized anti-virus management tools.

This report is intended solely for the use of the City of Milwaukee. Jefferson Wells does not take any responsibility for the reliance on this information by any external third parties.

Control Item – Patch Management:

Internal and external systems citywide varied to what extent they had been patched against vulnerabilities. With the increased number of computer worms and viruses in the last several years, this poses a risk to the City. Additionally there were no developed policies or procedures as to how, when and which patches are deployed, and in what timeframe.

Recommendations:

The City should develop standard policies and procedures establishing the time frame in which patches must be evaluated and deployed and a methodology to then deploy patches in a timely manner.

Control Item – Printer Security:

None of the departments/divisions had secured their network printers with a username/password combination. This creates a risk for the City in which any user can log on to the administrative interface for the network printer, manipulate the printer, and potentially capture other users' print jobs.

Recommendations:

All network printers' administrative interface should be secured with a username/password combination.

Control Item – E-mail Access:

At the time of the assessment, several departments/divisions had different electronic mail configurations. This includes running completely different e-mail systems, with e-mail gateways on different Internet connections, different operating systems ("OS"), and different e-mail server applications. With the increase in e-mail viruses and worms over the last several years, the current architecture allows for multiple entry points into the City network.

Recommendations:

The City should standardize on a common e-mail platform with a centralized system of email gateways. This would allow for greater security and monitoring of e-mail entering the City systems. Additionally this would provide a technology and cost savings, as technicians would only have one common email platform to support. It would also reduce the number of disparate email servers on the network.

This report is intended solely for the use of the City of Milwaukee. Jefferson Wells does not take any responsibility for the reliance on this information by any external third parties.

Security Layer #5 – Platforms

Overview and General Observations

The "Platforms" security layer refers to operating system level controls. Operating system control areas often include standardization, change control, patch management, event logging, auditing, lockdown procedures, and access controls. Platform controls are critical when addressing the security and risks of a major application that reside on a platform. For example, a web server application is loaded on a server, which runs on a particular operating system. Procedures are then followed to lock down the web server application according to manufacturer or industry specifications. The security concern is that the operating system, which the web server is running on, may be an "out of the box" installation, with many known vulnerabilities. The end result is that this server may be compromised. Applying security configurations approved by the City results in "hardened" or more secure platforms.

During the assessment, the following general observations were noted:

- In larger departments/divisions, standardized hardening procedures were generally utilized. Some of the smaller departments/divisions have not hardened their systems.
- Most departments/divisions stated they utilized group-based access rights.

Areas for Security Controls Enhancement

During the assessment, the following areas for controls enhancement were identified:

Control Item – Password Policies:
Citywide policy dictates that passwords are to be at least six characters long, not easily guessable, and have at least one non-alphabet character. While the majority of interviewed departments/divisions were following these standards on primary platforms, such as Microsoft and Novell, platforms on other devices, such as printers and network equipment, were noted to have less stringent policies. Some of these devices were found to have minimal or no passwords enforced.

Approximately half of the departments/divisions interviewed regularly changed administrative passwords. Similarly, approximately half the departments/divisions reported that their administrators did not have separate day-to-day accounts to use for non-administrative functions.

This report is intended solely for the use of the City of Milwaukee. Jefferson Wells does not take any responsibility for the reliance on this information by any external third parties.

Recommendations:

While based on interviews, it appeared most departments/divisions were following the password standards defined by citywide policy. It is recommended that the City review its current policy and consider revising it to the following:

- Passwords should be as many characters as feasible for the specific platform, database, or application (e.g., a minimum of six characters)
- Passwords should be forced to use a combination of alphanumeric characters
- Where feasible, passwords should be forced to contain at least one special character
- Passwords should be forced to change based upon the role of the end-user and the relative risks of his/her password being compromised (e.g., a minimum of 45 days for all userids and fewer days for userids with security administrative rights)
- Re-use of at least the last five passwords should not be allowed

Password policies are often considered a first line of defense and therefore, rules for password use must be standardized and enforced throughout all City departments/divisions. Password policies must be enforced on all network devices and platforms that have authentication enabled. Reminders of the password policy should be communicated to all users periodically to stress the importance of choosing passwords carefully and keeping passwords confidential.

The City should consider developing and implementing a policy regarding the changing of administrative passwords on servers and other networked devices. The policy should require that administrative passwords should be changed at least semi-annually and immediately upon termination, for cause or not for cause, of any employee with access to such accounts.

The City should require that all administrative users have separate network accounts and system administration accounts. While this may appear to be an inconvenience, there are risks that should be addressed. The inevitability of human error can pose a high risk to the organization. Accidental changes, deletions, or overwriting of files pose a higher risk and can be more difficult to detect with a system administration account.

Control Items – Event Logging and Review Procedures:

Most departments/divisions interviewed stated that event logging was enabled on key systems, however, only half of the departments/divisions claimed to review these logs on a consistent basis. Current City policy states, "each department/division shall document and track security related events and transactions." These records "must be maintained by ISO's for a period of six (6) months."

Recommendations:

City policy should consider adding definitions of minimum levels of logging for all departments/divisions and standards for log review and reporting. The CSO should be responsible for enforcing these defined policies throughout all departments/divisions.

This report is intended solely for the use of the City of Milwaukee. Jefferson Wells does not take any responsibility for the reliance on this information by any external third parties.

Security Layer #6 – Workstations

Overview and General Observations

The "Workstations" security layer consists of both physical and technical controls in place on department/division workstations and peripherals, including removable media and personal digital assistants ("PDAs"). With today's use of client/server technology, local workstations and many peripherals can contain sensitive information which must be protected with the same level of importance as data located on network servers. PDAs are utilized to synchronize employees' calendars and emails, as well as have the ability of storing word processing documents and spreadsheets. Small and portable hard drives are becoming more commonly used. These drives can be small enough to put on a key chain and hold upwards of 256Mb of data. Many of these devices are now incorporated within cellular phones, which without explicit policies can be difficult to control. The possible methods of an employee or attacker being able to retrieve or remove data with these technologies are constantly increasing.

During the assessment, the following general observations were noted:

- Most departments/divisions had adequate inventories of workstations within their departments/divisions, including asset tag numbers and the users assigned to them.
- Change control procedures for workstation patch management were observed as lacking formalization. (Please see the Security Layer # 1 control and recommendations regarding change control for additional information.)

Areas for Security Controls Enhancement

During the assessment, the following areas for controls enhancement were identified:

Control Items – Password Protected Screensavers:
The City Information Security Policies and Standards states, "Network-connected workstations must always be logged off or secured when left unattended." Through the interview process, approximately half of the interviewed departments/divisions stated they have controls in place to force automatic usage of screensaver passwords. One noted obstacle to the implementation of automatic screensavers was in departments/divisions that were still operating on Windows 9x/Me operating systems.

Recommendations:
Automatic usage of screensaver passwords should be implemented on all workstations throughout all City departments/divisions. Minimum recommended timeout settings for the screensavers should be set at a management-defined timeframe, e.g., at fifteen minutes. Departments/divisions running operating systems such as Windows 9x/Me should evaluate migrating such machines to Windows 2000/XP operating systems. The importance of locking unattended workstations should be covered in required user security awareness training.

This report is intended solely for the use of the City of Milwaukee. Jefferson Wells does not take any responsibility for the reliance on this information by any external third parties.

Control Item – Polices and Controls on Removable Media and PDA Devices:
Of the nine departments/divisions interviewed, only two departments/divisions reported having some level of controls in place to restrict the access of removable media, such as floppy disks, ZIP, USB hard drives, CD-ROMs, and cellular phones. Of the nine departments/divisions, only three stated having additional controls in place regarding the use of PDAs.

Recommendations:
With the ever-increasing use of PDAs, wireless devices, USB hard drives and cellular phones, it has become difficult to control how data can be brought into and out of an organization. These devices have been developed to provide users easy access to information from almost anywhere. When the possibilities of such communications are introduced to a network, the risks of exposing confidential information increase dramatically.

The City should perform a formal citywide assessment on the use of PDAs and other portable devices within the City network and the current controls in place to protect the City from improper uses and unnecessary risks associated with such devices. Upon review of the information gathered in that assessment, the City should define policies and standards that specifically state how such devices are permitted to be used and what additional controls need to be implemented to reduce the level of risk to an acceptable level.

Control Item – Workstation Re-use Policies and Procedures:
Workstation re-use policies and procedures refer to the steps taken by the IT department/division when an employee leaves the department/division and that user's workstation is redeployed to another employee. Of the nine departments/divisions interviewed, approximately half of the departments/divisions stated that they followed some form of process regarding the re-deployment of workstations. Only a couple departments/divisions actually had formal documented procedures.

Recommendations:
The City should develop minimum guidelines for all departments/divisions that define the steps to follow when re-deploying a workstation. Points to consider for these guidelines includes, but not limited to:

- Is data on the workstation properly reviewed and backed up before re-formatting drive?
- If the possibility of legal issues is apparent after a termination, were the proper steps performed when backing up the hard drive to ensure and document "chain of custody?"
- Is the workstation hard drive completely rebuilt or re-imaged before the workstation is redeployed?

This report is intended solely for the use of the City of Milwaukee. Jefferson Wells does not take any responsibility for the reliance on this information by any external third parties.

Security Layer #7 – Databases

Overview and General Observations

The "Database" security layer concentrates on technical controls in place to ensure the confidentiality, integrity, and availability of critical application databases. For the purpose of this "Defense-in-Depth" assessment, database controls were only addressed at a high-level. Database controls can be complex and vary based on the associated operating platform, database vendor, and the level of customization involved. Therefore the questions asked in the interview process were cursory related to the level of controls in place.

During the assessment, we observed that most of the major databases discussed in the interviews were documented and backup plans did exist.

Areas for Security Controls Enhancement

During the assessment, the following areas for controls enhancement were identified:

Control Item – Database Audits and Assessments:

It was noted through the interview process that a considerable number of database applications exist throughout the various departments/divisions. The controls and levels of documentation for each of these databases vary from department to department. Most of the departments/divisions interviewed reported that periodic database audits and vulnerability assessments were not being performed.

Recommendations:

It is understandable that it may not be always practical or cost-effective to set standards and policies that are applicable to all of the various database systems used citywide. Therefore, the City should first perform a citywide discovery assessment, with the goal of developing a comprehensive listing of all database systems throughout the city departments/divisions. This list should be used to create a "database security classification model" based on the value and confidentiality of the data, as well as the inherent risk levels associated. With this classification, the City can develop an audit and vulnerability assessment plan to verify the proper controls are in place and working effectively over time.

This report is intended solely for the use of the City of Milwaukee. Jefferson Wells does not take any responsibility for the reliance on this information by any external third parties.

Security Layer #8 – Data

Overview and General Observations

"Data" security assessments entail addressing controls such as data classification, access controls, retention and disposal, data flow, and monitoring access.

During the assessment, the following general observations were noted:

- Throughout the interview process it was noted that some departments/divisions had formal procedures in place for data classification and access controls, while some did not.
- The primary area of focus for recommendations to enhance security controls is the development and implementation of data classification procedures.

Areas for Security Controls Enhancement

During the assessment, the following areas for controls enhancement were identified:

Control Item – Data Classification:
Approximately half of the interviewed departments/divisions stated they have policies and/or procedures and a process for data classification including the formal assignment of data security roles. About half of these departments/divisions stated they have policies and procedures in place restricting the transmittal of data based on data classification levels.

Recommendations:
The City should develop citywide policies and procedures, defining the minimum standards to be followed by all departments/divisions regarding the formal classification of data. With these minimum standards in place, individual departments/divisions should be required to formulate their own formal policies and procedures for data classification, taking into consideration that some departments/divisions will require more stringent controls based on the data housed.

The CSO should evaluate the department/division policies to ensure the level of controls established is adequate for the data in question and that the documentation meets the minimum standards established by the City. These policies and procedures should define the roles and responsibilities of the staff involved in the process and include the controls established for monitoring the effectiveness of these controls.

Based on the classification level of the data within each department/division, each department/division should then formally define the standards to be followed when handling or transmitting the data. Particular concern should be placed on any type of transmittal of confidential data across public networks such as the Internet. Access controls should be developed, based upon the levels of classification. The theory of "minimum necessary" should be the basis of who has access to what information. This

This report is intended solely for the use of the City of Milwaukee. Jefferson Wells does not take any responsibility for the reliance on this information by any external third parties.

means that each user should only be allowed access to the minimum amount of data necessary for the job to be performed. Without the initial step of data classification, implementing "minimum necessary" access controls is difficult, if not impossible to achieve. Once the data classification system and standards are in place, each department/division should have periodic audits performed to ensure practices follow the developed standards.

This report is intended solely for the use of the City of Milwaukee. Jefferson Wells does not take any responsibility for the reliance on this information by any external third parties.

Security Layer #9 – Applications

Overview and General Observations

The "Application" security layer consists of controls in place at the business application level. Application level controls assessed include application criticality analyses, data edits and controls, application access controls, and application development.

During the assessment, the following general observation was noted:

- While in practice, the majority of the departments/divisions interviewed appeared to have an understanding of the controls in place to monitor and control applications, few of the departments/divisions have taken the next step of formalizing policies and procedures or documentation of such controls.

Areas for Security Controls Enhancement

During the assessment, the following areas for controls enhancement were identified:

Control Item – Application Criticality Analysis:
Approximately half of the interviewed departments/divisions stated they have performed an application criticality analysis.

Recommendations:
An application criticality analysis should be performed within each city department/division. This analysis will be the basis by which additional application risks and controls assessments should be performed. The analysis should in turn be repeated and updated on a periodic basis, at least annually.

The application criticality analysis is an essential tool for departments/divisions to formally document the applications within its business environment. There are different methods of performing such an analysis, each having their own advantages and disadvantages. An effective application criticality analysis should consider, but not necessarily be limited to the following:

- System name
- System owner
- Hardware and software requirements
- Application use description, including what data is accessed based on level of confidentiality.
- Interconnectivity and dependencies with other applications and systems.
- Departmental and interdepartmental user dependencies on application.
- System operating and downtime costs
- Internal and external support staff requirements

This report is intended solely for the use of the City of Milwaukee. Jefferson Wells does not take any responsibility for the reliance on this information by any external third parties.

Based on the results of this analysis, applications should be ranked by importance within the department/division and citywide. Additional assessments should then be performed on the application controls of the systems based on criticality. The application criticality analysis is also a required step in the development of the departmental business recovery planning, recommended in Layer #1 of this report.

Control Item – Software Inventories and License Audits:
Of the nine departments/divisions interviewed, half of the departments/divisions stated they perform formal software inventories and have some level of software licensing audits performed on at least an annual basis.

Recommendations:
Similar to the application criticality analysis, formally documented software inventories are a necessary step in the development and maintenance of a business recovery plan. Each department/division should maintain an accurate and up-to-date inventory of all software within the departments/divisions. On at least an annual basis, the departments/divisions should have a formal software license audit performed to ensure the accuracy of the inventory and legal compliance with vendor licensing agreements and with copyrighted products.

Control Item – Web Server Audits and Application Development Lifecycle:
Of the nine departments/divisions interviewed, four of the departments/divisions stated they have documented application development lifecycle procedures in place. This is critical when dealing with web servers. A few of the departments stated they have department/division web servers exposed to the public Internet. It is to be noted however, that upon department/division network scanning performed, more web servers were noted then accounted for. This often is due to server operating system installations that are not hardened to baseline procedures. Many times web servers are loaded with default installations of server operating systems. These default web server installations are inherently insecure.

Recommendations:
All web servers, especially those exposed to the Internet, should be developed and maintained within the guidelines of a formal application development lifecycle policy and procedure.

An application development lifecycle, sometimes called "system development life cycle (SDLC), is a conceptual model, used in project management, that describes the stages involved in an information system development project, from an initial feasibility study through maintenance of the completed application. Application development lifecycle policies and procedures should minimally include the following:

- Evaluation of existing system
- Definition of new system requirements
- Design and development of new system
- Testing, including documented test results
- Implementation of system into production
- System maintenance
- Audits and Assessments.

This report is intended solely for the use of the City of Milwaukee. Jefferson Wells does not take any responsibility for the reliance on this information by any external third parties.

Security Layer #10 – People

Overview and General Observations

Throughout the Defense-in-Depth model, the flow of the layers 'begins and ends' with "People." Policies and procedures are the guidance and standards the City defines for its system users to follow. Arguably, people are often considered an organization's greatest asset and, conversely, its greatest risk.

During this risk assessment, the following general observations were noted:

- Most departments/divisions interviewed stated background and reference checks are performed on all employees.
- The three primary areas addressed in this report for the "people" layer are regarding security policy, security awareness training, and vendor management.

Areas for Security Controls Enhancement

During the assessment, the following areas for controls enhancement were identified:

Control Item – Security Policy and Awareness Training:
Of the nine departments/divisions interviewed, only two of the departments/divisions stated that all end users are required to sign a security policy prior to gaining access to the network and only one department stated that users go through some level of security awareness training.

Recommendations:
Citywide policy, or Common Council resolution, should require all users read and sign an information security policy prior to being allowed access to network systems. On at least an annual basis, each user should again be required to re-read the policy and sign that they have read it and understand what it is saying. Documentation of the policies and the signed forms should be maintained in the users' personnel file. This requirement should not be restricted to City employees and elected and/or appointed individuals, but to all persons with a network account, including contractors and vendors. This policy and practice should be strictly enforced by the department/division security officials and ultimately by the CSO.

All users with access to the City information systems should be required to attend security awareness training. This training should be an ongoing process and should be repeated on a periodic basis, at least annually. Records of attendance should be maintained along with the documented training materials. Training should be developed based on the roles performed by the individuals. Department/division managers may not require the same level of training as IT staff. Individual departments/divisions should develop and implement supplemental training for its department/division users, focusing on unique security concerns encountered in the department/division.

This report is intended solely for the use of the City of Milwaukee. Jefferson Wells does not take any responsibility for the reliance on this information by any external third parties.

Control Item – Vendor Management:

Vendor management policies and procedures varied among the departments/divisions interviewed. Some of the departments/divisions had strict policies and controls in place, while others had no formal controls in place. A citywide policy or standard for vendor management was not apparent.

Recommendations:

The City should consider developing and implementing a citywide policy and standard for controls to evaluate and monitor outside vendors' access to City systems. These policies and standards should define the baseline controls by which all departments/divisions should comply. In turn, it should be required that each department/division develop and document, as necessary, additional standards and controls specifically relating to their department/division.

Addressable areas to consider in vendor management policies are:

- Pre-contract evaluation process including competitive analyses
- Documented needs and cost analyses for services provided
- Evaluation of vendors' security practices and controls
- Ensure vendors have performed background checks on all employees who may have access to City systems
- Formal contract with provisions relating to security and confidentiality of City information
- Logging and monitoring of vendors' physical access to the City facilities and logical access to the City network
- All non-City devices must be formally assessed, prior to connection to the City network, to ensure that anti-virus software and software patch levels are configured to reduce risks of virus infiltration or unauthorized activities to the City network

This report is intended solely for the use of the City of Milwaukee. Jefferson Wells does not take any responsibility for the reliance on this information by any external third parties.

Other Risk Assessment Engagement Deliverables

Deliverables from this security risk assessment for the City of Milwaukee included the items listed below. All of the deliverables were presented directly and completely to the Internal Audit – Audit Supervisor for audit use and secure storage. Future distribution of the engagement findings, observations, and other related data to any/all City department/division managers and/or IT personnel will be under the specific direction and control of the Comptroller's Office of the City of Milwaukee.

Deliverables related to overall City-level risk assessment and data analyses include a project binder containing:

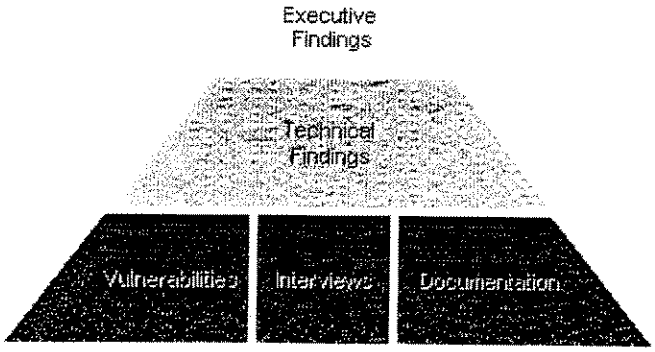
- Project charter
- Presentation materials
- Security Risk Assessment Report

Deliverables related to department/division-level risk assessments and data analyses include CDs containing the following department/division level documentation.

- City department/division contacts
- Project information request
- Network discovery information request
- Information Protection Architecture Risk Assessment ("IPARA") systems' profile forms
- Questionnaire worksheets
- Network scanning reports
- Supplied documentation from department/division
- Additional findings and observations

The technical security scans were performed within nine City departments/divisions using the Internet Security Systems vendor product Internet Scanner™ (version 7.0 at update level XPU 28). Corresponding Microsoft SQL databases from each scan session and product reports were generated for Internal Audit's use and secure storage. In the provided reports, three specific types of results could have appeared: Vulnerabilities, Technical Findings, and Executive Findings.

This report is intended solely for the use of the City of Milwaukee. Jefferson Wells does not take any responsibility for the reliance on this information by any external third parties.



Vulnerabilities are identified by the scans and listed in detail in the scan reports, they are also described across each area of the assessment. Vulnerabilities are classified higher-risk, medium-risk and lower-risk. Higher-risk vulnerabilities may provide unauthorized access to the host or to the network. As such, each one should be considered highly serious and should be dealt with as quickly as possible. Medium-risk and lower-risk vulnerabilities may provide access to network data that may lead to further exploitation.

Technical findings are the product of analyses of discovered vulnerabilities as well as interviews and review of collected technical documentation and exhibits. The findings are intended to assist technical management and staff with risk reduction efforts.

Executive findings are discussed in an Executive Summary section of the scan reports. The findings reflect a distillation of technical findings as they relate to business practices and contained high-level observations and recommendations. The executive findings are also intended to serve as the framework for a comprehensive security remediation plan.

This report is intended solely for the use of the City of Milwaukee. Jefferson Wells does not take any responsibility for the reliance on this information by any external third parties.

IT Audit "Roadmap"

Suggested IT Security Audits for the Comptroller's Office

As a deliverable of this security risk assessment, the Comptroller's Office requested Jefferson Wells to provide a suggested "list" of IT audits to perform based upon identified findings and observations. The list represents a combination of process, technical, City departments/divisions, and application controls' audits.

This list provided below is compiled as of a 'point-in-time.' In addition, due to the limited scope of this Security Risk Assessment engagement, the limited number of City departments/divisions included within the engagement scope, the lack of complete and/or accurate documentation from the "in-scope" departments/divisions, and the inability to detect all potential technical risks to the City's information assets, the list of audits is not to be considered comprehensive or prioritized.

Essentially Jefferson Wells is providing a "roadmap" for future IT security audits. We believe that there may be other IT audits listed if a more in-depth security risk assessment of all City departments/divisions had been performed, and/or if other areas of IT general controls (e.g., business continuity planning, systems development, computer operations, change management, and IT strategic planning) were included within the scope of a more comprehensive IT risks assessment.

Suggested IT Audit Areas

*Priority Legend	
A	Within a 1 year period
B	Within a 2 year period
C	Within a 3 year period

Audit / Assessment Name	Citywide Audit	Dept./Div. Audit	Priority*	Recommended Repeat Cycle
Technical Security Control Audits				
Firewall(s) Audit	√	√	A	Semi-annual
Internal Network Security Audit	√	√	A	Semi-annual
Network Penetration Test	√	√	B	Two year cycle
Remote Access (War Dial) Audit	√	√	B	Two year cycle
Web Server / Application Audits	√	√	A	Annual
Wireless Network Controls Audit	√	√	B	Two year cycle
Operating System Platform Audits (Microsoft Windows, Novell Netware, Unix, Mainframe)	√	√	B	Two year cycle
Database Controls Audits (SQL, Oracle, Dbase, Access)	√	√	B	Two year cycle

This report is intended solely for the use of the City of Milwaukee. Jefferson Wells does not take any responsibility for the reliance on this information by any external third parties.

Audit / Assessment Name	Citywide Audit	Dept./Div. Audit	Priority*	Recommended Repeat Cycle
Application Criticality Analysis	√	√	B	Two year cycle
Critical Application Audits (based on Application Criticality Analysis)	√	√	A	Annual
PeopleSoft Application Audit	√		B	Two year cycle
Email System Audit	√	√	C	Three year cycle
Anti-virus Controls Audit	√	√	C	Three year cycle
Emergency Response "911" System Audit		√	B	Two year cycle
Intrusion Detection / Incident Response Audit	√	√	A	Annual
Physical Security Audit	√	√	A	Annual
Change Control / SDLC Audit	√	√	B	Two year cycle
Disaster Recovery Audit	√		B	Two year cycle
Department / Division Security Control Audits				
In-depth Security Controls Audit of ITMD		√	C	Three year cycle
In-depth Security Controls Audit of MPD		√	C	Three year cycle
In-depth Security Controls Audit of MFD		√	C	Three year cycle
In-depth Security Controls Audit of DPW		√	C	Three year cycle
High-level Security Controls Audits of Departments / Divisions not included in this assessment		√	C	Three year cycle

As each audit's formal scope and budget is estimated, factors that will impact the audit process include the number and availability of City personnel to interview; the number and complexity of systems and applications to assess for control risks and vulnerabilities; the number of identified weaknesses that need detailed analysis and detailed definition of remediation options; department/division management's perspective of risk tolerance within its applications and technical infrastructure; potential legal and/or regulatory issues; availability of requested business, application, operational, and technical documentation; and availability of City resources to assist the audit team.

The recommended repeat cycle for audits listed in the table are based on the current state of risk faced by the City in the areas addressed. Long-term frequency of such audits may be adjusted, at the City's discretion, based on the results of the future audits and formalized policies and control procedures implemented to mitigate risks.

End of Report.

City of Milwaukee

Department of Administration
Information and Technology
Management Division

Tom Barrett
Mayor

Sharon D. Robinson
Administration Director

Randolf A. Gschwind
Chief Information Officer

April 15, 2005

W. Martin Morics
City Comptroller
200 E. Wells Street, Room 404
Milwaukee, Wisconsin 53202

RE: City of Milwaukee Information Technology Security Risk Assessment

Dear Mr. Morics:

Thank you for the opportunity to comment on the "Information Technology Security Risk Assessment" audit, dated April 2005. The audit sheds light on the current risks surrounding information systems security in the City's decentralized IT environment.

While a comprehensive document of "Information Security Policies and Standards" was issued by DOA in 1996, they have generally not been followed by departments, nor enforced in any meaningful way. These standards and policies need to be comprehensively reviewed by an inter-departmental team and revised to reflect current risks and standards. This will be done under the direction of DOA-ITMD.

In addition, a comprehensive security architecture needs to be defined for the City, with departmental input. The Mayor, Director of Administration and Chief Information Officer are committed to ensuring the security of City systems and information.

It is important to note, as mentioned in the audit, that a restructuring of IT governance has recently been approved by the Mayor and Common Council. This initiative establishes a more unified governance structure that will provide a strategic direction for IT and improved coordination of IT efforts. The impact on security will be positive through the establishment of IT policies, standards and guidelines with departmental participation, and monitoring and enforcement by DOA.

The new ordinance also states that the Chief Information Officer (in DOA) shall "coordinate city network services by developing a citywide plan for network management, operations and policies in conjunction with the department of public works." This activity has already started, and should result in better network security through coordinated management of city network equipment and constant proactive monitoring of network activity and traffic.

A critical component of security not to be overlooked is improved and effective training, not only for technical personnel, but for all employees who use City systems. Every City employee must use positive security practices in their work to ensure the integrity of the systems they access. Such practices also need to be monitored and enforced systematically.

We will work with the Mayor and Common Council to define a security architecture, policies and standards that are both cost-effective and avoid risks to City information.

Sincerely,

Sharon Robinson

Sharon D. Robinson
Director of Administration

Randolf A. Gschwind

Randolf A. Gschwind
Chief Information Officer

Copy: Mayor Tom Barrett
Alderman Willie L. Hines, Jr.
Alderman Michael Murphy

City of Milwaukee

Department of Public Works

Jeffrey J. Mantes
Commissioner of Public Works

James P. Purko
Director of Operations

April 15, 2005

Mr. W. Martin Morics
City Comptroller
City Hall, Room 404

Re: DPW Response to the City of Milwaukee Information Technology Security Risk Assessment Audit

Dear Mr. Morics:

We appreciate the opportunity to respond to the City of Milwaukee Information Technology Security Risk Assessment Audit. The Department of Public Works (DPW) comments are provided below.

As you know, DPW is responsible for designing, supporting and maintaining the community wide area network serving the departments of Police, Fire, Public Works, Water, Health, Neighborhood Services, Library and the Port of Milwaukee data communication needs. For DPW security is not an academic exercise but a 7/24/365 responsibility to defend public health and safety operations from daily attacks. DPW wants to assure the departments we serve that the community wide area network is extremely secure and that security risks are held to a minimum. DPW will continue to balance security risks and operational needs without compromising service delivery and creating cumbersome procedures that diminish our ability to provide responsive and cost effective network services. However, DPW does agree that there should be an overall security policy that incorporates every aspect of information technology. We will work with the Department of Administration to develop such policies and procedures that will enhance security efforts for all aspects of information technology across the City.

The information technology budget for the DPW-Administration Division reflects a number of City wide functions, which is not accurately reflected in Exhibit 2. This Division supports the community wide area network for 85% of all network traffic in City government. No other department has this level of responsibility. In addition, this staff supports all voice communications including landline and wireless communications. This responsibility is also unique only to this division. It is our opinion that given the responsibility for voice and data communications for most of City government, information technology provided by the DPW-Administration Division is extremely cost efficient and effective.

We appreciate the opportunity to respond to the audit report. If you have any questions, please contact Dorinda Floyd, Administrative Services Director, at 286-5582.

Very truly yours,

Jeff J Mantes

Jeffrey J. Mantes
Commissioner of Public Works

JJM:DRF:ph

c: Dorinda Floyd
Gerry Froh
Kenneth Walker
File