Board of Commissioners of Cook County

Report of the Technology Committee

Tuesday, June 17, 2014 11:15 AM **Cook County Building, Board Room, Room 569**
118 North Clark Street, Chicago, Illinois

SECTION 1

ATTENDANCE

Present: Chairman Fritchey, Vice Chairman Gorman, Commissioners Butler, Daley, García, Goslin, Schneider, Silvestri and Steele (9)

Absent: None (0)

Also Present: Commissioner Murphy, Simona Rollinson, – Chief Information Officer; Dorothy Brown – Clerk of the Circuit Court; Bridget A. Dancy – Chief Information Officer, Office of the Clerk of the Circuit Court; Mary Jo Horace – Deputy Chief Information Officer; Tom Lynch – Director of ERP; Robert McInerney – Chief Information Officer, Office of the Sheriff; Douglas MacClean – Deputy Director, Office of the State's Attorney

PUBLIC TESTIMONY

Chairman Fritchey asked the Secretary to the Board to call upon the registered public speakers, in accordance with Cook County Code, Sec. 2-107(dd).

1. George Blakemore, Concerned Citizen

14-1411

Presented by: Simona Rollinson, Chief Information Officer, Bureau of Technology

REPORT
Department: Cook County Bureau of Technology
Request: Refer to the Committee on Technology
Report Title: Quarterly Progress Report on the Creation of the Automated Criminal Justice System
Report Period: 3/1/2014 - 5/31/2014
Summary: Pursuant to Resolution 13-2002, the CIO shall update the Board of Commissioners via the Technology Committee on progress being made towards achieving the goal of an integrated, automated Cook County Criminal Justice System on a quarterly basis beginning with the first quarter of the FY2014. This is the second quarterly report of FY2014.

A motion was made by Commissioner Silvestri, seconded by Commissioner Steele, that this Report be recommended for receiving and filing. The motion carried by the following vote:

Aye: Chairman Fritchey, Vice Chairman Gorman, Commissioners Butler, Daley, García, Goslin, Schneider, Silvestri and Steele (9)

Presented by: Mary Jo Horace, Deputy Chief Information Officer, Bureau of Technology

Sponsored by: JOHN A. FRITCHEY, County Commissioner and TONI PRECKWINKLE, President, Cook County Board of Commissioners

PROPOSED ORDINANCE

COOK COUNTY INFORMATION SECURITY ORDINANCE

WHEREAS, technology and information resources in the various agencies and departments of Cook County are strategic and vital assets belonging to the people of the County; and

WHEREAS, Cook County government has a duty to its citizens to ensure that the information entrusted to its agencies is safe, secure, and protected from unauthorized access, use, or destruction; and

WHEREAS, coordinated efforts are necessary to protect these assets against unauthorized access, disclosure, use, and modification or destruction, whether accidental or deliberate, as well as to assure the confidentiality, integrity, and availability of information; and

WHEREAS, a strong information security framework must be coordinated, promulgated and implemented throughout county agencies and departments, including the offices of the separately Elected Officials, to ensure the development and maintenance of minimum information security controls to protect technology and information resources that support the operations and assets of said agencies and departments and to enable the County's protection of the public health, safety, morals and welfare;

NOW THEREFORE BE IT ORDAINED, by the Cook County Board of Commissioners that Chapter 2 Administration, Article I, In General, Division 1, Cook County Information Security, Sec. 2-8 through 2-14 of the Cook County Code, is hereby enacted as follows:

ARTICLE I. In General

Division 1 Cook County Information Security

Sec. 2-8. Short title.

This division shall be known and may be cited as the "Cook County Information Security Ordinance."

Sec. 2-9. Purpose and Policy.

All Elected Officials, Departments, Office Institutions or Agencies of Cook County ("County"), including but not limited to the offices and departments under the jurisdiction of the County Board President, the Board of Commissioners, Cook County Health and Hospitals System, Cook County State's Attorney, Cook County Sheriff, Cook County Public Defender, Clerk of the Circuit Court of Cook County, Cook County Treasurer, Cook County Clerk, Cook County Recorder of Deeds, Cook County Assessor, Chief Judge of the Circuit Court of Cook County, Board of Review, Cook County Public Defender, Independent Inspector General, Veteran's Assistance Commission and the Public Administrator (collectively, "County Agency") shall take all reasonable precautions to protect the confidentiality, integrity, and availability of County information. Such precautions shall be in

accordance with applicable Federal and State laws and regulations and take into consideration industry standards and best practices.

Sec. 2-10. Definitions.

The following words, terms and phrases, when used in this division shall have the meanings ascribed to them in this section, except where the context clearly indicates a different meaning:

Guideline means a recommendation to assist a County employee or County contractor in making appropriate decisions or performing a particular task, which allows for latitude in interpretation and implementation. *Plan* means a comprehensive document that details strategic direction, which may also provide additional details, such as Standards used and so forth.

Policy means a document that communicates leadership expectations to an organization or business unit, which may also be considered as mandatory business rules or organization-specific directives and which are communication of management intent.

Procedure means a document stating the manner in which a Policy shall be functionally implemented in a County Agency's environment, which may define specific operation steps, manual methods, or instructions for compliance with a Policy.

Standard means a document that contains a specification or describes minimum implementation that satisfies a Policy.

Sec. 2-11. Information Security Framework.

(a) Subject to the approval of the Cook County Chief Information Officer ("CIO"), the Bureau of Technology's Chief Information Security Officer ("CISO") shall create comprehensive and written information security Plans, Policies, Procedures, Standards, and Guidelines for the County and County Agencies (collectively, the "Information Security Framework") to reasonably protect the confidentiality, integrity, and availability of County information; all County Agencies shall collaborate with the CISO in the creation of the Information Security Framework as requested.

(b) The Information Security Framework shall be in accordance with applicable Federal and State laws and regulations and take into consideration industry standards and best practices.

(c) The Information Security Framework shall include a risk management process, which the CISO shall direct, to identify information security risks in County Agencies and deploy risk mitigation strategies, processes, and procedures.

(d) The Information Security Framework shall include information security incident and breach response Plans as a subset of information security.

Sec. 2-12. Adoption and Compliance

(a) The CIO and CISO shall publish and make available the Information Security Framework to all County Agencies; said County Agencies shall adopt and comply with the Information Security Framework.

(b) County Agencies may deviate from the Information Security Framework based on their unique requirements, but only upon receiving prior written approval from the CIO and CISO.

(c) County Agencies shall take all appropriate actions, including completing assigned training and if warranted, initiating disciplinary action, to ensure their employees and contractors adopt and comply with the Information Security Framework.

Sec. 2-13. Review, Remediation and Enforcement

(a) Annually the CISO shall review and approve the proposed information security Plans of each County Agency to determine if such Plans are in conformance with the Information Security Framework or properly deviated with prior written approval from the CIO and CISO.

(b) Annually the CISO shall review the status of County Agency adoption and compliance with the Information Security Framework and timely report compliance related issues to the CIO.

(c) Where a County Agency has not fully adopted or complied with the Information Security Framework, the CIO and CISO shall direct that County Agency to take the necessary remediation steps and other measures required for adoption and to bring them into compliance.

(d) The CIO and CISO shall be authorized to take all appropriate actions to ensure and enforce compliance with the Information Security Framework.

Sec. 2-14. Reporting and Exceptions.

(a) At least once each calendar year, the CISO through the CIO shall report to the Cook County Board of Commissioners on the Information Security Framework.

(b) At a minimum, the CISO's annual report shall detail: (i) the status of all County Agencies' adoption and compliance with the Information Security Framework and (ii) a summary of all requests for deviations from the Information Security Framework that the CISO has previously approved or rejected.

Effective date: This ordinance shall be in effect immediately upon adoption

A motion was made by Commissioner Daley, seconded by Commissioner Gorman, that the substitute to Item 14-1481 be recommended for acceptance. The motion carried by the following vote:

Aye: Chairman Fritchey, Vice Chairman Gorman, Commissioners Butler, Daley, García, Goslin, Schneider, Silvestri and Steele (9)

Sponsored by: TONI PRECKWINKLE, President, Cook County Board of Commissioners and JOHN A. FRITCHEY, Commissioner, Cook County Board of Commissioners

PROPOSED SUBSTITUTE ORDINANCE FOR FILE ID 14-1481

COOK COUNTY INFORMATION SECURITY ORDINANCE

WHEREAS, technology and information resources in the various agencies and departments funded by the Cook County Board of Commissioners are strategic and vital assets belonging to the people of the County and State; and

WHEREAS, Cook County has a responsibility to the citizens of Cook County to ensure that the information entrusted to these agencies is safe, secure, and protected from unauthorized access, use, or destruction; and

WHEREAS, coordinated efforts are encouraged to protect these assets against unauthorized access, disclosure, use, and modification or destruction, whether accidental or deliberate, as well as to assure the confidentiality, integrity, and availability of information; and

WHEREAS, a strong information security framework should be coordinated, promulgated and implemented throughout agencies funded by the County, including the offices of the separately elected County and State Officials, to ensure the development and maintenance of minimum information security controls to protect technology and information resources that support the operations and assets of said agencies and departments and to enable the protection of the public health, safety, morals and welfare.

NOW THEREFORE BE IT ORDAINED, by the Cook County Board of Commissioners that Chapter 2 Administration, Article XII, Cook County Information Security Ordinance, Sec. 2-960 through 2-967 of the Cook County Code, is hereby enacted as follows:

ARTICLE XII. Cook County Information Security

Sec. 2-960. Short title.

This article shall be known and may be cited as the "Cook County Information Security Ordinance."

Sec. 2-961. Purpose and Policy.

All separately elected County and State Officials, Departments, Office Institutions or Agencies funded by the Cook County Board of Commissioners, including but not limited to the offices and departments under the control of the County Board President, the Board of Commissioners, Cook County Health and Hospitals System, State's Attorney of Cook County, Cook County Sheriff, Cook County Public Defender, Illinois Clerk of the Circuit Court of Cook County, Cook County Treasurer, Cook County Clerk, Cook County Recorder of Deeds, Cook County Assessor, Chief Judge of the Circuit Court of Cook County, Board of Review, Cook County Public Defender, Cook County Independent Inspector General, Cook County Veteran's Assistance Commission and the Public Administrator (collectively, "Agency") shall take all appropriate precautions to protect the confidentiality, integrity, and availability of information. Such precautions shall be in accordance with applicable Federal and State laws and regulations and take into consideration industry standards and best practices.

Sec. 2-962. Countywide Information Security Working Group.

(a) An Information Security Working Group shall be composed of the directors of the information systems for all Agencies set forth in Section 2-961, or the directors' designees.

(b) The Bureau of Technology's Chief Information Security Officer ("CISO") shall be the chair of the Information Security Working Group.

Sec. 2-963. Definitions.

The following words, terms and phrases, when used in this article shall have the meanings ascribed to them in this section, except where the context clearly indicates a different meaning:

Guideline means a recommendation to assist an Agency employee or contractor in making appropriate decisions or performing a particular task, which allows for latitude in interpretation and implementation.

Plan means a comprehensive document that details strategic direction, which may also provide additional details, such as Standards used and so forth.

Policy means a document that communicates leadership expectations to a business unit or department of an Agency, which may also be considered as mandatory business rules or organization-specific directives and which are communication of management intent.

Procedure means a document stating the manner in which a Policy shall be functionally implemented in an Agency's environment, which may define specific operation steps, manual methods, or instructions for compliance with a Policy.

Standard means a document that contains a specification or describes minimum implementation that satisfies a Policy.

Sec. 2-964. Information Security Framework.

(a) The Information Security Working Group shall assist the CISO in creating, and updating as necessary, comprehensive and written information security Plans, Policies, Procedures, Standards, and Guidelines for the Agencies (collectively, the "Information Security Framework") to reasonably protect the confidentiality, integrity, and availability of Agency information.

(b) In creating and updating the Information Security Framework, the CISO shall seek the advice and recommendations of each Agency in order to ensure that the Information Security Framework addresses unique considerations of said Agency; all Agencies shall advise and collaborate with the CISO in the creation of the Information Security Framework.

(c) The Information Security Framework shall: (1) be in accordance with applicable Federal and State laws and regulations; (2) state all Agencies' minimum requirements and precautions to protect the confidentiality, integrity, and availability of Agencies' information; (3) address the unique considerations of each Agency in a manner that does not unduly interfere with the operations of such Agency or any confidentiality or privilege required for such operations; and (4) take into consideration industry standards and best practices by including critical and necessary components of any such similar framework, for example, risk management processes, information security incident response plans, and data breach notification plans.

Sec. 2-965. Adoption and Compliance

(a) The Bureau of Technology's Chief Information Officer ("CIO") and CISO shall publish and make available the Information Security Framework to all Agencies; said Agencies shall adopt and comply with the Information Security Framework in a reasonable time, except as set forth in subsections (b) and (c) of this section. The CIO, CISO and Agencies shall not otherwise disclose the Information Security Framework except as required to further the security of the various information systems or as required by law.
(b) After publication of the Information Security Framework, Agencies may deviate from the Information Security Framework based on their unique requirements, but only upon the approval of the Information Security Working Group and signing of a mutual agreement that would be executed by the CISO and the Agency following the Information Security Working Group approval.

(c) After publication of the Information Security Framework, any Agency not under the control of the County Board President may elect to not adopt and comply with the Information Security Framework by sending written notice to the CIO, the Chair of the Information Security Working Group, and the Technology Committee of the Board of Commissioners within ninety calendar days after such publication; provided that to the extent that such Agency continues to use or access information systems under the management or control of the CIO, the CIO may only allow such Agency to use and access such information systems in a manner consistent with the use and access conditions of the Information Security Framework.

(1) Any Agency not under the control of the County Board President that elects to not adopt and comply with the Information Security Framework under this subsection may, subsequently and at any time, elect to adopt and comply with the Information Security Framework by giving written notice ninety calendar days' in advance to the CIO, the Chair of the Information Security Working Group, and the Technology Committee of the Board of Commissioners.

(2) The adoption and compliance with the Information Security Framework, or the lack thereof, shall not affect any rights and responsibilities arising under any law, including the Illinois Constitution, the Illinois Counties Code, or the Code of Ordinance of Cook County, Illinois.

(d) Agencies adopting the Information Security Framework shall take all appropriate actions, including completing assigned training and if warranted, initiating disciplinary action, to ensure their employees and contractors adopt and comply with the Information Security Framework.

Sec. 2-966. Review, Remediation and Enforcement

(a) No less than annually, the CISO shall review and determine the status of Agency adoption and compliance with the Information Security Framework and whether an Agency's use and access of County information systems adheres to the use and access conditions of the Information Security Framework.

(b) Where the CISO has determined that an Agency has not fully adopted or complied with, or uses or access County information systems contrary to, the Information Security Framework, the CIO and CISO shall notify the Information Security Working Group and that Agency to remediate such deficiencies in adoption, compliance, use or access in a reasonable time; and the CISO shall assist such Agency with its remediation effort if requested.

(c) The CIO and CISO shall be authorized to take all other appropriate actions to protect the County's network that are consistent with the requirements of the Information Security Framework.

(d) Where an Agency disagrees with the CISO's determination that such Agency has not fully adopted or complied with, or uses or access County information systems contrary to, the Information Security Framework, then such Agency may request that the Information Security Working Group review and determine the status of such Agency's adoption and compliance with the Information Security Framework. The CISO shall follow the Information Security Working Group's determinations.

Sec. 2-967. Reporting.

(a) At least once each calendar year, the CISO shall report to the Information Security Working Group on the Information Security Framework.

(b) At a minimum, the CISO's annual report shall detail: (i) the status of all Agencies' adoption and compliance with the Information Security Framework, and (ii) a summary of all advice and recommendations of each Agency regarding their unique considerations. Based on information provided by the Information Security Working Group, the CISO may modify his or her annual report.

(c) The CIO shall present the CISO's annual report to the Cook County Board of Commissioners following the presentation of that report to the Information Security Working Group.

Effective date: This Ordinance shall be effective upon passage.

A motion was made by Commissioner Butler, seconded by Commissioner Schneider, that Item 14-1481 be recommended for approval as substituted. The motion carried by the following vote:

Aye: Chairman Fritchey, Vice Chairman Gorman, Commissioners Butler, Daley, García, Goslin, Schneider, Silvestri and Steele (9)

14-2269

Presented by: Mary Jo Horace, Deputy Chief Information Officer**,** Bureau of Technology
PROPOSED CONTRACT (TECHNOLOGY)
Department: Bureau of Technology
Vendor: SunGard Availability Services LP, Wayne, Pennsylvania
Request: Authorization for the Chief Procurement Officer to enter into and execute.
Goods or Services: Information Security, Compliance and Incident Response Services
Contract Value: $1,364,123.00
Contract period: 7/1/2014 - 6/30/2018~~5/1/2014 - 4/30/2018~~, with two (2) two-year extension options
Potential Fiscal Year Budget Impact: FY2014 $171,659.00~~$228,443.00~~; FY2015: $340,704.00; FY2016: $340,704.00; FY2017: $340,704.00; FY2018: $170,352.00~~$113,568.00~~
Accounts: 769-260 Account
Contract Number: 1350-12461
Concurrences:
The Vendor has met the Minority and Women Owned Business Enterprises Ordinance..

The Chief Procurement Officer Concurs

Summary: In 2013, Cook County issued an RFP for Information Security, Compliance and Incident Response services, which resulted in the contract that BOT now seeks authorization for the CPO to execute. Procuring the services of information security experts is a critical step to improving the County's information security practices, achieving compliance with applicable information security regulations and best practices, and properly handling information security incidents.

Cook County provides services for approximately 5.3 million residents. Many of these services handle sensitive information including social security numbers, credit card numbers, and personal health information. With the assistance of information security consulting experts, the County can enhance its information security program by performing nationally recognized risk assessments, enhancing the County's information security framework, performing additional cyber security monitoring and testing, and improving its incident response and forensic response capabilities. In addition to the objectives identified above, other desired outcomes include the protection personal information of County residents and the mitigation of cyber-security risks.

A motion was made by Commissioner Butler, seconded by Commissioner Schneider, that this Contract (Technology) be recommended for approval as amended. The motion carried by the following vote:

Aye: Chairman Fritchey, Vice Chairman Gorman, Commissioners Butler, Daley, García, Goslin, Schneider, Silvestri and Steele (9)

14-3173

Presented by: F. Thomas Lynch, Director, Enterprise Resource Planning (ERP)
REPORT
Department: ERP, Enterprise Resource Planning
Request: Refer to Committee on Technology
Report Title: ERP Project Status Report
Report Period: Ongoing

Summary: The Director of ERP will provide a comprehensive update to the Board of Commissioners via the Technology Committee on the status of all ongoing ERP projects. The status update will reflect progress being made towards achieving the goals of selecting and implementing a Countywide Enterprise Resource Planning (ERP) platform, configuring and installing a biometric-based Time & Attendance system, and upgrading and migrating the JDEdwards HR/Payroll system to a cloud hosting environment. This is the first report of FY 2014.

A motion was made by Commissioner Gorman, seconded by Commissioner Schneider, that this Report be recommended for receiving and filing. The motion carried by the following vote:

Aye: Chairman Fritchey, Vice Chairman Gorman, Commissioners Butler, Daley, García, Goslin, Schneider, Silvestri and Steele (9)

ADJOURNMENT

Commissioner Daley, seconded by Commissioner Gorman, moved to adjourn the meeting. The motion passed and the meeting was adjourned.

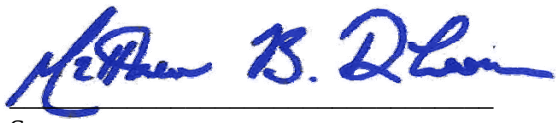
SECTION 2

YOUR COMMITTEE RECOMMENDS THE FOLLOWING ACTION WITH REGARD TO THE MATTER NAMED HEREIN:

File Id14-1411	Recommended for Receiving and Filing
File Id14-1481	Recommended for Approval as Substituted
File Id14-2269	Recommended for Approval as Amended
File Id14-3173	Recommended for Receiving and Filing

Respectfully submitted,

Chairman



Secretary

*A video recording of this meeting is available at https://cook-county.legistar.com