NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES

INFORMATION TECHNOLOGY EXAM RESULTS FOR THE NEW YORK STATE COMMON RETIREMENT FUND

AUGUST 20, 2013

I. Executive Summary

The essential components of the Common Retirement Fund's ("CRF") technology infrastructure are old, outdated, and out of support. The mainframe system is more than 25 years old. It is written in a programming language that was created in 1959 and in which few programmers are still trained. During our exam, two key operating systems were beyond their manufacturer's support date so they no longer were being updated to protect against ever-evolving security threats. CRF executives acknowledged that the antiquated Information Technology ("IT") system was a major risk for the CRF, that the system is approaching a point of failure, and that the CRF has been aware of these problems for years. A failure would be devastating for New Yorkers that rely on the system to handle their private information and to administer and distribute their retirement savings.

In addition to an antiquated system, the CRF's IT disaster recovery plans are inadequate. The designated data recovery and business continuity sites are both too close to the CRF's headquarters, the disaster recovery plans are not thorough, and disaster recovery testing is not adequately performed. The lack of disaster recovery planning puts the retirement systems' vital data at an even greater risk in the event of a disaster or system failure.

The serious IT failures that exist at the CRF might have been mitigated or corrected if IT audits had occurred regularly and recommendations been monitored. IT audits of the CRF do not happen frequently enough and, when they do occur, their recommendations are not adequately tracked. Without audit tracking, the CRF fails to implement the recommendations it receives from the rare IT audits that occur. An audit tracking policy, which includes proper review and oversight, should be put in place as soon as possible.

The deficiencies in the CRF's technology infrastructure, disaster recovery planning, and IT auditing would create significant risks for any large institution, particularly a nearly $160 billion public pension system that holds the highly sensitive information and important assets of many New Yorkers. The CRF has not taken adequate steps to address these deficiencies. They must be addressed immediately.

II. Background

The Superintendent of the Department of Financial Services ("DFS") supervises New York State's actuarially funded public retirement systems. N.Y. Retire. & Soc. Sec. Law § 15. As part of this authority, he has the power to require annual reports on matters he prescribes, to

promulgate standards, and to examine "the affairs" of every retirement system, at least every five years. N.Y. Ins. Law § 314(b). The Superintendent regularly examines all public retirement systems regulated by DFS, including those comprising the CRF.[1] These exams are conducted pursuant to N.Y. Insurance Regulation No. 85, 11 N.Y.C.R.R. § 136-2, and they observe the guidelines established by the Government Accounting Standards Board, an independent organization that establishes standards of accounting and financial reporting for U.S. state and local governments, and by the Actuarial Standards Board, that promulgates actuarial standards some of which govern actuarial methods and assumptions used by public employee retirement systems.

In 2012, DFS undertook an exam of the CRF for the five-year period from April 1, 2006 through March 31, 2011. The CRF exam included a review of governance and enterprise risk management, accounts and records, financial statements, investment issues, actuarial issues, member benefits, and information technology.

The IT portion of the exam, the results of which are summarized in this report,[2] focused on the IT risk management processes and included a review of audit coverage, management policies and oversight, controls in development and acquisition of software and hardware, and support and delivery functions.[3] The objective of this portion of the risk-based exam was to identify, understand, and assess organization-wide business risks created by IT. The IT exam included a questionnaire response, on-site interviews over multiple days, document collection and review, and a review of the data center and the disaster recovery centers. The exam was led by an experienced examiner, with over 25 years' IT experience.

A. IT Management Structure at the CRF

[1] The NYS Employees' Retirement System and the NYS Police and Fire Retirement System, are known collectively as New York State and Local Retirement Systems ("NYSLRS") and their assets are combined for investment purposes into the CRF. Participating employers in NYSLRS include New York State, local governments in the state (cities other than New York City, towns, villages, etc.), and local police and fire districts.

[2] DFS notified the CRF of the findings of this report on August 7, 2013. Under New York Insurance law § 311(b)(1),(2), (c), within ten days of such a notice, the entity subject to an examination may request a hearing on the report before its publication. The CRF did not request a hearing.

[3] As DFS has previously stated publicly, it intends to issue a series of reports on individual subjects of concern at New York State's public pension funds (both across the State and in New York City) – rather than just publishing a single report on each fund. DFS believes that this new approach will help provide stronger oversight and improve accountability at those funds by more clearly highlighting specific issues that deserve prompt corrective action. Previously, the Insurance Department – DFS's predecessor agency – wrote a single report on each fund and only published those reports periodically. As DFS has previously stated, it believes that it is in the public interest – for both taxpayers and public employees – to strengthen oversight of New York's public pension funds, given that those funds hold hundreds of billions of dollars in investments and provide retirement benefits for millions of New Yorkers.

The Division of the Chief Information Officer ("CIO") provides IT services throughout the Office of State Comptroller ("OSC"), especially with respect to the major business applications and the information technology infrastructure. Among these business applications is the Member, Employer, Benefits, Executive, and Legal ("MEBEL") application. There is not a separate IT department dedicated to the management of MEBEL or the IT needs of the retirement system. The CIO, Kevin Belden, reports to the First Deputy Comptroller who reports directly to the Comptroller, who is the sole trustee of the CRF and has control of and is directly accountable for its performance, oversight, and management. *See* N.Y. Retire. Soc. Sec. Law §§ 15, 315, 177.

B. Core Functions CRF's IT System Must Support

The MEBEL application is the information system that supports the core business processes of the retirement system including benefits processing, calculating and payment, employer billing and reporting, and enrollment and termination of memberships. It also provides several supporting business functions that are essential to the CRF's core business functions such as actuarial calculations, security functions, document management, financial management, and workflow management.[4] The system processes more than one million transactions per month for member salary and service credit calculations alone.[5] This information system is, according to the OSC's internal auditor, "one of the top ten mission-critical government systems in New York State."[6]

MEBEL operates in an IBM mainframe environment and was created for the OSC in 1987 with support from Anderson Consulting. DB2, a relational database management system from IBM, is the underlying database for the MEBEL application and the SQL Server, a Microsoft database management system, is used to store, retrieve, and process data. IBM z/O.S. is the operating system for MEBEL. MEBEL is written in the programming language COBOL (Common Business-Oriented Language) and interfaces using CICS (Customer Information Control System) which is a transaction server that supports online transaction processing.[7]

III. Findings of the Exam

A. Information Technology Infrastructure is Outdated and Must be Replaced

The essential components of the CRF's technology infrastructure, including its primary processing platform, operating system, and software, are old, outdated, and out of support, creating a substantial and potentially dangerous problem for the system. Should this antiquated

[4] N.Y. State Office of the Comptroller, RFP 11-03, Pension Administration System Modernization, November 10, 2011.

[5] Response to IT Planning Questionnaire Question 3(d).

[6] November 8, 2011, Office of Internal Audit Memo, "Platforms and Technology Unit and Service Delivery Unit" (Engagement #09-07).

[7] Response to IT Planning Questionnaire Question 3(d).

IT system fail, the system may not be able to meet the CRF's goal of "secur[ing] retirement benefits to enable members, retirees and beneficiaries to plan for a more financially secure retirement, and protect[ing] the assets of the system."[8] Indeed, executives of the CRF acknowledged during our examination that its IT systems are a major risk, are "approaching a point of failure" and that the limitations in their technological systems render it unable to "fully achiev[e] NYSERS' strategic goals."[9] Response to IT Planning Questionnaire Question 3(d). The deficiencies in the CRF's technology infrastructure are imprudent for any large institution, particularly a nearly $160 billion public pension system that holds the highly sensitive information and important assets of many New Yorkers. These deficiencies must be addressed immediately.

a. Mainframe Core Processing System Is Over 25 Years Old

Using a system that is more than 25 years old for such a high volume of transactions is dangerous, particularly because the systems and programs MEBEL was intended to interface with are also now very outdated and there are a small and dwindling number of specialists able to use and maintain them.[10]

MEBEL is written in the programming language COBOL (Common Business-Oriented Language) and uses CICS (Customer Information Control System) which is a transaction server that supports online transaction processing. COBOL was created in 1959 and is one of the oldest programming languages. CICS was released in 1968. Both are very outdated. The CRF faces a serious problem as the availability of programmers proficient in both COBOL and CICS is small and will continue to deteriorate over time as new computer specialists are not being trained in these old systems and the COBOL/CICS specialists at the CRF approach retirement. *See* Response to ITPQ Question 3(d) (acknowledging that programming and technical experts on these programs are approaching retirement eligibility). CRF IT representatives acknowledged that they have faced difficulties "in finding and hiring mainframe programmers and technical staff" and that there is a learning curve of 18–24 months for new programming and technical hires to learn the CRF's systems. *Id.* This is particularly problematic because the CRF acknowledged that even with its current number of COBOL/CICS specialists, IT staff is unable "to react quickly to requests from business units for improved MEBEL functionality." *Id.* In addition, CRF has also acknowledged that it has "no 'in-house' expertise" for some of the programs that MEBEL uses. *Id.*

In addition to the lack of programmers who can use MEBEL, CRF employees also identified significant functionality problems with MEBEL that should be addressed, including the fact that it is not easily compatible with new technologies, does not have sufficient memory

[8] NYSLRS' Strategic Plan, Critical Success Factors, and Key Performance Indicators (cited in Request for Proposal, 11-03, Pension Administration System Modernization for New York State and Local Retirement Systems, November 10, 2011, at 44.

[9] CRF representatives have also admitted that the fund's technology has limitations that "affect" the ability of the fund to meet its goals. Memo No. 4, Responses to IT Review, 8/9/12.

[10] The CRF is in negotiations to engage a vendor to provide a replacement for MEBEL. Once the vendor is chosen, the actual process of replacing MEBEL will take several years.

capacity to house necessary information, may need to be reprogrammed in order to continue to function, and is difficult to use for data mining. *See Id*.

The CRF is only now beginning the process of replacing MEBEL. The replacement process should be accelerated and the new system should address the problems that both DFS examiners and CRF employees themselves have identified.

b. Operating System and Database Management System Were Beyond End-of-Support Date

CRF customized software, utilizing MEBEL, which is essential to the business of the CRF, was out of date during our examination. Its operating system[11], IBM's z/O.S., has not been supported since September 30, 2012 and will be out of date until a replacement that was scheduled for this year. Its database management system, SQL Server[12], which retrieves information from the CRF's database, such as important actuarial data, was out of support from July 2011 until it was upgraded in January 2013, several months after the DFS examination began.

Using software that is not supported creates serious security and business risks and contravenes best practices and industry standards. Software vendors do not create security patches or fixes for recently identified problems for software that is past their formal support end dates. This lack of security and functionality protection leaves the retirement system's data vulnerable to bugs and to security breaches, including attacks by hackers. Outdated software also lacks customer support, may become difficult to upgrade, and can create integration problems as other components in the technology architecture are updated.

The Federal Financial Institutions Examination Council ("FFIEC"), the intergovernmental agency that prescribes principles and standards for the federal examination of financial institutions, classifies "obsolescence of software (including loss of hardware or software support)" as a "technology investment mistake" that should be identified for risk identification and assessment management.[13]

OSC's own "Patch Management Standard" requires that its infrastructure components be "consistently patched enterprise-wide in order to protect OSC against known security threats." It further states that the "development, implementation, and ongoing maintenance of a vigorous patch management life-cycle program are essential requirements for risk mitigation and the management of a successful security program to ensure the effectiveness and security of OSC operational environment." It is impossible for the CRF to meet the OSC Patch Management Standard if it uses out-of-support software for which security patches are not issued.

---

[11] An operating system is a collection of software that manages computer hardware resources and provides common services for computer programs.

[12] The SQL Server is a software product whose primary function is to store and retrieve data as requested by other software applications.

[13] FFIEC IT Examination Handbook (August 2003), Operations Booklet, at pg. 9.

The use of out-of-support software creates serious risks. Because of this vulnerability, it is commonly understood among IT professionals that large institutions should not use out-of-support software. The CRF should replace its unsupported software at the earliest date possible and its IT policy should be changed to forbid the use of unsupported software.

c. The CRF Has Ignored Recommendations to Update Its IT Infrastructure

The replacement of MEBEL will take several years and should have begun years ago. Every year, from 2007 through 2011, the Division of Retirement Services identified IT risk as one of the most significant operational risks it faced. CRF IT management reported that, although the need to replace MEBEL and its related software has been known for some time, the replacement process has been halted by "higher-ups in the Comptroller's office." Interview of VanDeusen, and McPadden, 5/21/12.

B. Disaster Recovery Plans are Inadequate

The lack of disaster recovery planning endangers the safety and soundness of the CRF in the event of a disaster. The CRF's disaster recovery plans are not prudent because the designated data recovery and business continuity sites are both too close to the CRF's headquarters at 110 State Street in Albany, the disaster recovery plans are not thorough, and disaster recovery testing is not adequately performed.

The CRF plans to use either 90 State Street or Riverview Center (150 Broadway, Menands, NY) as a business continuity site where employees could work if the 110 State Street headquarters was not available in a disaster. Memo No. 4, Responses to IT Review, 8/9/12. 90 State Street is two buildings away from 110 State Street and Riverview Center is approximately three miles away. Both are too close to the headquarters to serve as an effective business continuity site. In the event of a disaster that impeded the use of the CRF headquarters, it is likely that surrounding buildings would also be unavailable for use. The CRF should designate a business continuity site that is a greater distance from its headquarters.

The CRF's designated data recovery site is its headquarters, 110 State Street, which is 6.5 miles from the primary data center at Rensselaer Technology Park. Memo No. 4, Responses to IT Review, 8/9/12. This is not far enough away to provide for an effective data recovery site because many disasters that would affect the primary data center would also affect the data recovery site. In addition, the 110 State Street location is not currently capable of replacing the primary data center. While there is adequate storage and equipment in the facility, the current HVAC capacity of the site is inadequate as there are not sufficient heat exchangers on the roof of the building to support any growth or increase in capacity. The CRF should establish an adequate data recovery site that is further away from its primary data center.

The CRF's disaster recovery plan does not include adequate procedures for recovering its operations, nor any articulation of baseline metrics required. For example, it does not include a recovery time objective (how long it will take to get the application running) and recovery point objective (to what point of time the application will be restored) for each of the CRF's applications. It does not contain procedures for recovering the processing capacity of the primary data center, which should be a priority in the event of a disaster. It also does not have a

complete Business Impact Analysis, a common tool that organizations use to predict consequences of disruption of business functions and processes and develops recovery strategies.

There is also no explicit policy for IT disaster recovery testing at the CRF and when any testing does occur, the results are not given to management or the board of directors. In fact, the CRF does not actually do *anything* that would normally be regarded as disaster recovery testing. For example, no testing is done of the recovery of processing capabilities for the primary data center at Rensselaer Technology Park. *Id.*

The CRF disaster recovery plans fail to meet the OSC's own "disaster recovery standard." OSC Disaster Recovery Standard. The standard requires that the OSC have a disaster recovery plan that "identifies and mitigates risks to systems and sensitive information and provides contingencies to restore information and systems in the event of a disaster." It specifically requires a risk assessment, identifying and ranking threats and vulnerabilities, and a Business Impact Analysis. The CRF does not have or update an effective risk assessment or Business Impact Analysis. It does not meet industry standards or OSC's own standard.

The disaster recovery process will be quicker and more efficient if it is planned and tested in advance. We recommend that the CRF create a thorough disaster recovery plan. It should include procedures for recovering capacity at the primary data center, list by priority which applications should be recovered, and list the recovery time objective and recovery point objective for each application. The CRF should also create an IT policy requiring annual testing of the disaster recovery plan and that the results be forwarded to the board of directors for review.

C. IT Audits Are Inadequate

IT audits of the CRF do not happen frequently enough. There is no defined cycle within which all elements of the IT audit universe are reviewed and/or audited and the IT portion of the annual audit plan is sparse, especially given that the audit plan is for the entire agency rather than specific to the CRF. There are only three IT internal auditors for the entire agency and IT-specific audits occur only 2–3 times a year agency-wide (so most are not related to the CRF). Indeed, although we requested IT audits from the previous year, the CRF had to go back several years to find 2–3 IT audits because of the infrequency by which IT audits are performed for the CRF.

Industry standards and best practices make clear that audit plans should not be open-ended. The FFIEC prescribes that written guidelines should specify a maximum length for audit cycles based on risk scores. Industry standards suggest that controls around key activities and primary security controls should be examined annually, and all aspects of the IT environment should be audited on a cycle of 3 to 5 years. We recommend that audit IT examinations occur on this firm cycle for all items in the IT audit universe including the security and operations of the data center and password policy compliance.

We also recommend that the CRF institute specific requirements for internal auditors. There are currently no set requirements for IT internal auditors at the CRF, such as an explicit requirement for a CISA or other formal certification or a specified type or amount of experience

or schooling. The "most qualified" candidate is chosen from applicants. The IT auditors currently employed at the OSC are not highly qualified. The two non-director IT auditors have no professional certifications and had no audit experience before joining the OSC.[14]

The tracking of IT audits is also inadequate. There is no formal audit tracking report or policy at the CRF. This contravenes accepted industry standards and best practices. Furthermore, the FFIEC prescribes that all audit programs should include "[f]ollow-up processes that require internal auditors to determine the disposition of any agreed-upon actions to correct significant deficiencies."[15]

While the Office of Internal Audit (OIA) reported that it monitors recommendations, the weakness of its ad-hoc system without a formal tracking policy can be seen in the OIA's own reports. For example, a July 13, 2010 OIA memo entitled "Follow-Up Review of Intrusion Testing of the Entire IT Infrastructure and the Portal Infrastructure (Audit #05-08)" was issued as follow-up nearly three years after an initial audit report on intrusion testing and states that:

> [A] majority of the recommendations have been either partially implemented or not implemented at all. As a result, there remains a level of risk to OSC's Enterprise Network infrastructure and Portal applications that has not been sufficiently mitigated. OIA believes that the assets within the OSC IT Infrastructure remain at an unacceptable risk of unauthorized access by external and internal parties.

Without audit tracking, the CRF fails to implement the recommendations it receives from the rare IT audits that occur. An audit tracking policy, which includes proper review and oversight, should be put in place as soon as possible.

The serious IT failures that exist at the CRF might have been mitigated or corrected if IT audits had occurred regularly and audit recommendations been monitored. In addition to addressing its major IT failures, the CRF must revise its IT audit polices to create controls that will prevent future failures.

IV. Conclusion

Information Technology is essential to the administration of New York's massive pension system. Despite this, the CRF has not prioritized the modernization and protection of its IT systems. Essential IT infrastructure components are outdated, there is not adequate disaster recovery planning, and IT auditing is not done regularly or effectively. These deficiencies create serious risks for the system. Failures in IT could lead to security breaches, the loss of private and sensitive information, the miscalculation of service credits and benefits, or inaccurate or delayed member payments. Any of these problems could be devastating to New Yorkers who depend on their pension payments for living expenses and who rely on the CRF to protect their sensitive information. Further, the occurrence of even the smallest error or security breach could become a massive and costly undertaking for a nearly $160 billion public pension system.

---

[14] Auditor Experience Summary Document.

[15] *See* FFIEC IT Examination Handbook (August 2003), Audit Booklet, at pg. 11-12.

The CRF must work to eliminate these IT deficiencies immediately. In particular, it must update the essential components of its IT infrastructure system, institute adequate disaster recovery, regularly audit its IT components, and track the implementation of audit recommendations. Putting these procedures in place will minimize the risk of an IT failure.

The Superintendent of DFS is also planning to introduce regulations to ensure that the CRF and other New York retirement systems actively monitor the suitability of their IT systems and protect against emerging risks. The regulations will require New York public pension systems to have IT governance, risk management, and internal controls in place to ensure IT systems are operated and maintained securely and efficiently. In particular, the regulation will require the adoption of policies to protect sensitive information; the appointment of an Information Security Officer; the establishment of an internal IT audit unit; and annual IT assessments, penetration testing, and disaster recovery testing.