New York State

and

Local Retirement System

Response to the Department of Financial Services Examination Report on Information Technology

August 23, 2013

Office of the State Comptroller
Thomas P. DiNapoli

New York State and
Local Retirement System
Kevin F. Murray, Executive
Deputy Comptroller

NEW YORK STATE AND LOCAL RETIREMENT SYSTEM
RESPONSE TO:

INFORMATION TECHNOLOGY EXAM RESULTS FOR THE NEW YORK STATE COMMON RETIREMENT FUND
AUGUST 20, 2013 [DFS Report]

The New York State and Local Retirement System (NYSLRS) provides this response to the Department of Financial Services (DFS) Report on the Information Technology Portion of an Examination of the New York State and Local Retirement System.

The examination report and press release from DFS contained numerous inaccuracies, misleading statements and errors. The fundamental lack of understanding of the distinction between NYSLRS' benefit administration functions and the investment activities of the Common Retirement Fund (CRF) and their relationship to the management and structure of the Comptroller's Office promotes undue concern for members, retirees and beneficiaries about the security of their pension information. We would like to make the following points:

1. *Retirement benefit information is safe.*
2. *The information systems discussed in this report are unrelated to the investment activities of the Common Retirement Fund (CRF).*
3. *The Retirement System has undertaken a disciplined process of benchmarking other retirement systems and identifying business process improvements.*
4. *The Retirement System is in the process of completely overhauling its retirement benefit administration information technology system as has been planned and in the works for several years.*

The Retirement System is run on a secure and battle-tested system written in COBOL, a very stable programming language that is extensively used throughout New York State government as well as by financial institutions throughout the world. It has been a reliable, safe and flexible system that has served members, retirees and users well for decades.

Beginning in April 2007, staff at the Office of the State Comptroller has been working to develop the next system of computer programs to manage NYSLRS for the coming decades. We have been deliberate in our process to avoid costly mistakes made by others while completing such a large system-wide transition. The lack of mention of any progress in this area by DFS is a glaring oversight.

Because of the haste with which DFS decided to release the examination, NYSLRS did not have a formal response in the report.

Rather than characterize the comments and recommendations made by DFS, this response sets out the text of each of the various sections of the DFS report and then follows each section with NYSLRS' comments in blue italicized text.

I. Executive Summary [DFS Report]

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.

***NYSLRS Response**:*

Although footnote 1 recognizes the distinction between the New York State and Local Retirement System (NYSLRS) and the Common Retirement Fund (CRF), this report repeatedly refers to the CRF when it should refer to NYSLRS. The assets of NYSLRS are held and invested in the CRF. The MEBEL system that is criticized in the DFS report supports the benefit administration related function of NYSLRS. MEBEL does not support the investment operations of the CRF and is not used by investment staff. For accuracy, all references to the CRF in this report should be changed to refer to NYSLRS. This is a fundamental error, which could have been avoided had the Department of Financial Services not rushed to publication before receiving NYSLRS' response.

The remaining assertions of the Executive Summary will be addressed in the sections which follow.

II. Background [DFS Report]

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.

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.

A. IT Management Structure at the CRF [DFS Report]

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.

***NYSLRS Response**:*

Again, the DFS report seems to reflect a misunderstanding of the basic structure and operations of the NYSLRS. The MEBEL application relates to the Comptroller's role as administrator of NYSLRS (Retirement and Social Security Law Section 11) and includes, for example, support for benefit processing and payment. The MEBEL application does not support the investment operations of the CRF in the discharge of the Comptroller's duties in the above-cited section 177 of the RSSL.

B. Core Functions CRF's IT System Must Support [DFS Report]

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]

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).

III. Findings of the Exam [DFS Report]

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 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.

NYSLRS Response:

NYSLRS has been addressing replacement of MEBEL in a disciplined and effective manner for more than six years.

- *Beginning in April 2007, NYSLRS began work with Deloitte Consulting LLP (partnering with L. R. Wechsler, Ltd. and Documentation Strategies) on the following activities:*

- ***Gain an understanding of, and document current NYSLRS "As Is" business processes and how these processes and the underlying data functions interact*** *– 119 sessions were conducted with subject matter experts resulting in 147 "As Is" process maps and 11 discussion documents (for processes that did not need a process map). Those maps and discussion documents detailed how business is conducted in NYSLRS today. The process maps also contain high-level details concerning the complexity of each process. They can be viewed in the previously provided document* ***RFP 11-03: Pension Administration System Modernization for NYSLRS (November 2011) (****hereafter referred to as RFP 11-03); Reference 16 Documentation of NYSLRS' Current Business Processes (Provision® Maps);*

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.

- ***Performed analyses of peer public retirement systems to learn how their processes enable them to successfully deliver services*** *– NYSLRS staff traveled to peer retirement systems in California, North Carolina, Georgia, and Michigan, as well as to the New York State Teachers' Retirement System. As part of these visits, the peer systems discussed their modernization projects, how they began, challenges they faced, lessons learned and best practices;*
- ***Identified improvements that could be made to NYSLRS business processes to improve customer satisfaction, service delivery, and processing efficiency*** *– NYSLRS held 14 sessions with approximately 80 staff subject matter experts and developed business process improvements. Over 600 improvement opportunities were identified and categorized into potential short-, medium- and long-term implementation solutions. Some short- and medium-term improvements have already been implemented in our legacy systems. In addition, all improvements were considered in developing the business requirements for RFP 11-03;*
- ***Developed comprehensive business requirements for implementing business process improvements in the proposed Replacement System*** *– Starting with potential business requirements provided by its consultants (requirements acquired through engagements with other retirement system clients), NYSLRS held 35 sessions with subject matter experts to validate, modify and develop new business requirements for the new Pension Administration System solution;*
- ***Developed and issued a Request for Information (RFI) (May 2008).*** *– An RFI was issued to share with the vendor community a high-level overview of NYSLRS' recent activities and vision for the future, provide NYSLRS an opportunity to ask questions to help in structuring an RFP, and to provide the vendor community an opportunity to react and comment on discrete business, technical and administrative requirements for possible inclusion in RFP 08-01;*
- ***Reviewed and assessed vendor comments to the RFI;***
- ***Developed, finalized and issued RFP 08-01 Pension Administration System Modernization (July 2008) -*** *Proposals were received from vendors to provide products and services to fulfill all requirements in the RFP. Upon review, NYSLRS exercised its right to not make an award.*
- ***Developed, finalized and issued RFP 08-05 Change Management Services (Phase 1b) (February 2008).*** *RFP 08-05 resulted in the engagement with a Change Management vendor (SMART Consulting) to provide guidance with the following activities:*
    - *Create an Organizational Readiness for Change Assessment;*
    - *Develop and Execute a Communications Strategy;*
    - *Develop a Leadership Action Plan;*
    - *Develop a Stakeholder Engagement Plan; and*
    - *Develop a Workforce Transition and Capability Transfer Plan;*

- *The deliverables from the SMART engagement can be viewed in the previously referenced document: RFP 11-03; See Reference 18 Change Management Analysis;*

- ***Developed, finalized and issued RFP 08-16 Quality Assurance/Independent Validation and Verification Services (November 2008).*** *Proposals were received from vendors to provide Quality Assurance/Independent Validation and Verification (QA/IV&V) services in support of RFP 08-01. Because of the decision not to make an award as a result of RFP-08-01, no award resulted from this procurement.*

NYSLRS chose to undertake additional preparatory work to better prepare us to move forward with our initiative to replace our legacy systems with a secure, modernized Pension Administration System. NYSLRS staff conducted the following activities:

- ***Enhanced the Requirements Traceability Matrix*** *- The business requirements contained in RFP 08-01 were supplemented with the most recent business requirements (e.g. new requirements resulting from Tiers 5 and 6) from NYSLRS' "as is" environment to ensure that ALL business requirements were accounted for in this RFP and in the future Line of Business (LOB solution). These business requirements can be found in RFP 11-03 Reference 12 RTM for Business Requirements;*
- ***Performed Data Classification*** *– All existing business processes were reviewed to classify them into one of four data classifications: Public, Internal Use Only, Confidential and Restricted Confidential. Based on the confidentiality, integrity and availability of the data in those business processes, controls were identified and provided to the business units for implementation and for inclusion as a requirement in RFP 11-03. See RFP 11-03 Reference 21 Data Classification and Controls for more information;*
- ***Continued Data Cleansing*** *– Technical and business staff continued working jointly to identify data cleansing opportunities and plan a course of action for their remediation;*
- ***Initiated a Member Folder Backfile Conversion*** *– The New York State Industries for the Disabled was engaged in November 2010 to scan and index nearly 2.1 million paper member folders stored in NYSLRS' storage facility. Scanning folders for active members was prioritized in order to facilitate the integration of electronic workflow and scanned images with the future Line of Business (LOB) solution. Folders for active members were scheduled to be completed in the first three years. Active folders were completed ahead of schedule in August, 2013. The remainder of the folders (for Inactive members and those who received Final Payments) is scheduled to be completed within the next three years;*
- ***Expanded our Employer Partnership Initiative –*** *In order to improve and streamline our services to our employers, NYSLRS expanded its web-based offerings. In May 2013 we fully converted all of our employers to a web-based reporting system, eliminating hardcopy and other media in favor of a secure internet solution. Additionally, we expanded our offerings in this secure venue to include all previously manual employer billing related business information exchanges in order to better protect the confidentiality of our members' data and to prepare our employers to conduct all of their retirement business with NYSLRS in this secure, web-based manner.*

- ***RFI 11-01 - Developed and issued a Request for information (RFI)*** *– An RFI was issued in January 2011 to share with the vendor community a high-level overview of NYSLRS' recent activities and vision for the future, provide NYSLRS an opportunity to ask questions to guide us in structuring our RFP, and to provide the vendor community an opportunity to react and comment on discrete business, technical and administrative requirements which may be included in the RFP;*
- ***Reviewed and assessed vendor comments to RFI 11-01****; and*
- ***Developed, finalized and issued RFP 11-03 Pension Administration System Modernization*** *(November 2011) - Proposals were received in late March 2012 from vendors to provide products and services to fulfill all requirements in the RFP; and*
- ***Developed, finalized and issued RFP 12-01 Quality Assurance Services*** *(September 2012). Proposals were received in November 2012 to provide Quality Assurance (QA) services in support of all products and services described in RFP 11-03; and*
- ***Awarded RFP 11-03*** *- A full evaluation of the Proposals to RFP 11-03 was conducted. In late November 2012, Accenture LLP was notified that they had been selected to fulfill the products and services described in RFP 11-03. Contract negotiations ensued, culminating in contract signing in late May 2013; and*
- ***Awarded RFP 12-01*** *- A full evaluation of the Proposals to RFP 12-01 was conducted. In February 2013, KPMG was notified that they had been selected to provide quality assurance services in support of the activities described in RFP 11-03. Contract negotiations ensued, culminating in contract signing in late May 2013;*

To further ensure our success in achieving the business, customer service, and technology improvements that NYSLRS seeks, a dedicated team of NYSLRS staff continues to be assembled for the Redesign Project to ensure sufficient administrative, business and technology resources.

a. Mainframe Core Processing System Is Over 25 Years Old [DFS Report]

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

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.

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 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*.

NYSLRS Response:

NYSLRS has had a stable information system in place, Member, Employer, Benefit, Executive and Legal or MEBEL, that is constantly maintained and updated. This system has been a reliable work horse. A stable computer system has a low risk of sudden and arbitrary failure.

COBOL is still used in many large enterprises, and as part of Enterprise Resource Planning (ERP) systems like State Payroll and the State's new Financial Services System. CICS is a leading transaction server. OSC does not use the 1960's versions of these programs, and the time of invention is irrelevant. None of the hardware or software used by the System is old. The mainframe was purchased in 2009 and the software is current.

Although MEBEL has limitations that affect our ability to reach some of our goals, we have adapted other technologies to help meet our customers' needs. We have built auxiliary systems on technologies such as FileNet and DB2 Connect, just as an ERP might require bolt-ons. The software (and hardware) is upgraded regularly and is no danger of arbitrarily ceasing to function. Therefore, there is no need to reprogram MEBEL in order for it to continue to function. There is no issue with memory or storage capacity. With regard to the difficulty in using the current system for data mining, our systems replacement plans include the implementation of a more robust data extraction and analysis tool to support advanced data mining.

While schools are no longer teaching COBOL and CICS, we have been successful at hiring transfer candidates with these skills and training IT staff in these technologies. As a result of consolidations of State agency IT functions, more programmers will be available in the short term on state lists and as transfer candidates. In fact, OSC's IT shop is viewed as a "destination of choice" due to its leading practices, governance and record of success.

Senior IT managers continuously assess the skills and abilities of the staff that support the existing mainframe system. Succession planning has been ongoing, with particular attention being given to likely attrition over the next few years. Documentation is being reviewed for accuracy and completeness, and cross training of staff is occurring as part of the daily job assignments and work activities. Additionally we maintain a staffing level at least two-persons deep for any critical technology, and perform succession planning to have three staff where turnover is anticipated.

While implementing changes in the existing technology can take longer than the same effort in a newer technology, all legislative mandates have been met within prescribed timeframes. Detailed work plans are developed to manage and implement other system improvements that support Retirement's business priorities.

Regarding DFS's comment that the CRF acknowledged that it has "no 'in-house' expertise" for some of the programs that MEBEL uses, there is only one architecture program where we do not have in-house expertise. NYSLRS has successfully engaged consultant support to assist us in the rare instance where modifications to this program have been required. The system is current and reliable and the data is secure and accessible.

[DFS Report]

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.

NYSLRS Response:

The statement that the CRF is only now beginning the process of replacing MEBEL is erroneous. As detailed in our response to Section III A above, NYSLRS developed and implemented a comprehensive plan to replace MEBEL and our legacy systems in such a way that leverages best practices for large-scale modernization projects, as well as the practical experiences of our peer retirement systems. These steps were discussed in our response to Memo #4, transmitted on September 5, 2012, and have been updated and summarized in the Procurement Summary for Replacing MEBEL in our response on pages 5 through 8, and in our MEBEL and Legacy System Project Plan and Update in our response on page 13.

b. Operating System and Database Management System Were Beyond End-of-Support Date [DFS Report]

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

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

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.

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.

***NYSLRS Response**:*

New York State and Local Retirement System (NYSLRS) information systems run in OSC's data center and technology environment. NYSLRS' primary information system, MEBEL, is a mainframe-based CICS/DB2/COBOL application. This legacy system, originally built in the mid-1980's, is comprised of a suite of mature, stable products evidenced by the greater than 99% up-time availability of our system. The Chief Information Officer staff provides a full complement of support services covering hardware, underlying systems software, as well as business-specific application support. NYSLRS works with Chief Information Officer staff to perform a progressive cost/benefit analysis of its software, upgrades and maintenance releases to determine a plan for maintaining the stability of its information system. NYSLRS keeps up to

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.

date on the most recent release/maintenance level(s) of software. However, for some products, the changes offered in the new release (i.e., web enablement) might not be relevant or may present compatibility issues. Our decision-making process weighs the benefits of running on a more current release against the expenditure of resources (time, money, human) and of introducing risk to a stable system. As a result of this conservative approach, a few products have run beyond their formal end-of-support date. In those instances, because of our experience with these products, we are confident that they will continue to run successfully as long as we don't change the environment in which they are running. For example, if ASF is currently meeting our business needs, but running unsupported, we would not anticipate any problems until or unless we upgrade CICS or z/OS. At that point, we would upgrade ASF, as well as the other components, in a coordinated upgrade plan.

The statement that, "This lack of security and functionality protection leaves the retirement system's data lack of security and functionality protection leaves the Retirement System's data "vulnerable to bugs and to security breaches, including attacks by hackers." is also inaccurate. The system is not directly accessible externally. Neither z/OS nor CICS is used to protect the MEBEL system. Multiple IT assets are used as a "defense in depth" best practice approach to security. Since 1999, The OSC Office of Internal Audit (OIA) has engaged outside experts periodically to perform intrusion testing and application security reviews for various projects and infrastructure changes. They also ask during their annual risk assessments whether there is a need for intrusion testing in the upcoming year. These reviews generally touch on a large scope of controls, such as change management, configuration management, password strength, patch management, firewall management, etc. Access controls for business users are reviewed by OIA's Operational Audit team during its audits of NYSLRS' business units.

In the situation where the vendors confirm that we have a compatibility problem in any area, we upgrade the necessary components to move forward. Where unsupported software exists, the option to upgrade to a supported level is available from the vendor. If that is not immediately feasible, we pay for additional support as needed.

As noted above, Accenture LLP has been engaged to replace its NYSLRS' legacy systems. This engagement includes a technology infrastructure assessment where we will assess the components of our proposed new solution, taking into consideration our existing hardware/software assets, and making decisions regarding future asset investments.

With regard to the recommendation that the NYSLRS should replace its unsupported software at the earliest date possible and its IT policy should be changed to forbid the use of unsupported software, having software that is not current does not mean that it is unsupported. Had it been necessary (for example, if the security software was not current, or software was truly "unsupported"), NYSLRS would have developed an emergency procurement. IBM software support is always available for purchase (either ad hoc or via extended maintenance). All MEBEL legacy-related software cited in the Audit is now current. IBM has changed their practice to issue updates yearly which makes it much easier to stay current. A policy that would always require supported software would be counter-productive and harmful because some inter-relationships between software at specific release levels are not certified, or do not work.

c. The CRF Has Ignored Recommendations to Update Its IT Infrastructure [DFS Report]

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.

NYSLRS Response:

As referenced earlier, NYSLRS began executing a strategic and deliberate plan to determine our business needs, identify improvements to our business processes by benchmarking other retirement systems, and plan the replacement of MEBEL several years ago. This plan has included a regular assessment of risk and corresponding development and execution of mitigation strategies to ensure a successful replacement effort. Dave Van Deusen and Laurie McPadden agree that neither of them made a statement 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."

A summary of our MEBEL and Legacy Replacement Project is outlined below:

New York State and Local Retirement System
MEBEL and Legacy Replacement Project
Summary and Update

- ***Redesign Project Start*** *- Project staff from both Accenture and KPMG began their respective engagements with NYSLRS on June 11, 2013.*
    - *Accenture has contracted with NYSLRS for a 48-month development engagement with a subsequent full 12-month warranty period;*
    - *KPMG will perform their QA services of this work for a 50-month period;*
- ***Current Redesign Project Status:*** *Redesign is currently in Phase 1 - a project mobilization and initiation phase which is primarily for establishing the governance and framework of project methodologies for the subsequent phases of the project, as well as for mobilizing and acclimating the consultant(s) staff to NYSLRS' environment.*
- ***Phased Implementation Plan for NYSLRS' Redesign Project****:*
    - *Phase 1: Initiation/Mobilization*
    - *Phase 2: Planning and System Design*
    - *Phase 3: Hardware and Software Installation and Configuration*
    - *Phase 4: System Development/Multiple High-Level Functional Rollouts (listed as proposed, to be confirmed during Phase 2)*

- *Employer Reporting and establishment of Technology Enablers*
- *Pension Payroll*
- *Member Functions*
- *Self-Service Functions on the web*

▪ *Phase 5: Warranty, Support and Transition*

B. Disaster Recovery Plans are Inadequate [DFS Report]

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.

***NYSLRS Response**:*

In terms of risk, it has been NYSLRS experience that our physical sites in the Northeast are most susceptible to weather-related outages, such as snowstorms, brown-outs and electrical storms, or routine building maintenance issues such as power disruptions or interior water leaks. The relative proximity of our State Street and Riverview sites provides us with the flexibility to quickly divert our workforce to an alternate site in the event of such a disruption. The nearness of the sites minimizes the difficulties and logistical problems of relocating staff to a more distant site. Another important part of our recovery plan is to store data, both business data and system recovery data, for the NYSLRS systems in an offsite storage facility – Iron Mountain, located in Kingston, New York. Should the incident be of a nature that all sites were rendered inaccessible,

our Business Continuity Plan calls on us to have key designated staff utilize laptops and remote connectivity to access their work resources.

NYSLRS' risk mitigation strategy described below includes maintaining an inventory of IT assets, site and network information and a significant presence of laptops in our workforce. This has enabled us to effectively maintain business continuity at our two State Street sites and our Riverview site in the face of non-regional disaster incidents.

Fully one-third of NYSLRS' business staff, including those who are designated as key staff for business continuity purposes, are equipped with laptops and remote-access capability. As new/replacement laptops are rolled out, staff are instructed on how to access OSC's network through a secure VPN from a remote network location. NYSLRS maintains an outside network connection to support testing this functionality as well as issuing semi-annual reminders and guidance to staff to test their devices from their home locations. Should our primary work location become unavailable, key staff are expected to access all of their work resources in from home and other alternate locations. OSC's VPN is robust, stable, and regularly supports OSC's entire telecommuting workforce, including nearly 100 NYSLRS' telecommuters on a weekly basis.

Further, NYSLRS maintains an inventory of IT assets and network capacity information to help management make informed decisions in the event of an incident that renders one or more of NYSLRS' staff locations unusable. This information includes an inventory of desktop/laptops deployed to NYSLRS' staff, including their physical locations, and network capacity information, per physical location, for BCP purposes.

With regard to the comment that the HVAC capacity of the data recovery 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 heat exchangers at the 110 State Street site were updated in June of 2013, as planned, addressing the issue and expanding capacity.

[DFS Report]

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.

NYSLRS Response:

OSC/NYSLRS has a Disaster Recovery plan in place, with stated recovery time objectives (five days for critical systems). NYSLRS has a secondary, "disaster recovery" mainframe located at 110 State Street. In addition, all data created at the Troy site on DASD and HSM tapes are fully replicated to DASD and HSM tapes at the 110 State Street location. This replication of data

affords NYSLRS the ability to utilize the disaster recovery mainframe in the event of a disaster and access the data which has been previously replicated at that location.

NYSLRS has a defined Recovery Time Objective (RTO) of five days and a Recovery Point Objective (RPO) of a half day. With regard to Recovery Point Objectives, each night NYSLRS performs two separate backups of data files (one before our nightly batch processing and one backup after our nightly batch processing). These backups provide us with two distinct recovery points each night, at different processing intervals, and afford us the ability to recover quickly and seamlessly in the event of processing issues or a disaster scenario. In a recent test, OSC was able to fail over from our data center to our recovery site in approximately three hours, clearly meeting our RTO of five days. Similarly, OSC was able to recover our data to within mere minutes of a sync point, clearly meeting our RPO of a half day.

With respect to HVAC issues at our primary data center, Turner Construction has signed a contract with the Landlord of our Troy Data Center for a complete refurbishment project. The OSC has been working with Sigma 7 for over a year on the data center specifications. NYSLRS has also been working with the Chief Information Officer on a risk management business schedule.

All refurbishment work will be completed by the end of 2014, at which time OSC will have a Tier 3 level data center (i.e. Tier 3 is a level of data center availability that is defined by the National Uptime Institute that will provide OSC with increased levels of stability and availability that will support the high availability standards that NYSLRS is building our replacement system to achieve). Our risks are mitigated sooner, because the HVAC at our data center will have been replaced by the summer of 2014. Meanwhile, environmental risks at the current data center continue to be mitigated with maintenance contracts and mandated testing.

NYSLRS has done business impact analysis for years. However, the OSC recently purchased a Recovery Planner product as part of its plan for continuously improving business continuity planning that includes a Business Impact Analysis tool, which NYSLRS is utilizing to enhance its existing business impact analysis.

[DFS Report]

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.*

NYSLRS Response:

The statement that NYSLRS does not actually do anything that would normally be regarded as disaster recovery testing is completely inaccurate. OSC/NYSLRS is one of very few New York State agencies with a data center backup/disaster recovery capability of any kind. While there have been discussions among the executive agencies for many years about the need for IT disaster recovery capability, OSC/NYSLRS has taken affirmative action, and has had a backup

data center for more than two decades. We are acutely aware of the risks and implications of a disaster, and have put considerable resources into building a disaster recovery capability appropriate to the risk.

Testing has also been done to demonstrate the ability to confirm different connections as well as the integrity of the data copies. A recently performed test dictated that the Troy mainframe connection to the data was intentionally disrupted so as to provide no way to access the data stored in Troy. A secondary connection to the data stored at 110 State Street was engaged and processes were successfully executed by the Troy mainframe, while accessing the data copies at 110 State Street. The processes executed were not only confirmation of a solid alternative connection, but also provided a confirmation of the data integrity of the copies at the alternate location. The System restores tapes from our offsite back up storage at Iron Mountain (distance). A more expansive test which will include some more ancillary systems is planned for the fall of 2013. We are licensed by IBM to perform disaster recovery testing and plan to exercise our plan twice a year.

In 2004, OSC engaged Keane, Inc. to study the IT recovery strategies available to OSC and to make recommendations based on their findings. Keane investigated different recovery options:

1) Hot-Site;
2) Quick Ship;
3) Redundant/Mirrored Site;
4) Mobile Recovery Center; and
5) Alternate Recovery Facility

Based on their review, Keane recommended that the best option was the development of the redundant/mirrored site at 110 State Street. The Capital District region of New York is at a low risk for regional disasters such as earthquakes, tsunamis, and hurricanes. The threat caused by a disaster that would impact the power grid is mitigated by the existence of diesel generators at both sites. While the use of 110 State Street as a redundant site is our primary DR plan, we also have drop-ship agreements for additional equipment, as needed. Results of disaster recovery tests are reported to NYSLRS executive management upon completion of the testing and also regularly discussed at monthly meetings with NYSLRS executive management and the Chief Information Officer. There is no board of directors.

[DFS Report]

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.

***NYSLRS Response**:*

NYSLRS regularly conducts critical testing of disaster recovery capabilities. The most important regularly planned test is the semi-annual test of the ability to produce Pension and Advance Payroll disbursements at our recovery facility at the Department of Tax and Finance, consistent with long-standing practice and agreement. Our disaster recovery testing includes the ability to create both monthly pension disbursements and monthly advance disbursements in check form. We also create printed check registers and bank disbursement files related to the checks.

Results of the check printing tests are reported to NYSLRS executive management and the Chief Information Officer. This test provides assurance that in the event of a disaster, NYSLRS will be able to make retirement payments timely, using the most recent pre-disaster payroll files, while IT staff rebuilds the NYSLRS IT environment at the recovery site.

For pension disbursements, NYSLRS has two separate agreements with JP Morgan Chase, one for checks, the other for electronic funds transfer. These agreements protect NYSLRS' pensioners so that they are never at risk of not receiving their funds.

Having also tested our ability to connect the primary and recovery sites through multiple paths to access backup data at 110 State Street, and with a clone of our primary mainframe computer already in place at the recovery site, we are confident that we can recover critical NYSLRS systems within the stated five-day recovery time objective.

NYSLRS regularly updates their Emergency Management, Business Continuity, and Disaster Recovery plans. The critical system requirements (including MEBEL) are documented. An exhaustive list would not impact MEBEL recovery.

C. IT Audits Are Inadequate [DFS Report]

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.

NYSLRS Response:

The Office of Internal Audit (OIA) has issued 14 formal IT audit reports during the audit period of these examinations, seven of which either focus directly on NYSLRS or have a significant impact on them (agency-wide IT audits). These audits included wide-scope reviews such as intrusion testing and application security reviews for various projects and infrastructure changes, which generally touch on a large scope of controls, such as change management, configuration management, password strength, patch management, firewall management, etc. The OIA currently has two broad-scope IT audits in process, one of which impacts NYSLRS (IT Governance). OIA has provided assistance regarding IT controls and security through other activities in addition to IT audits, including:

- *Consulting engagements to assist NYSLRS before applications or internal controls are implemented, and during RFP processes.*
- *Advisory work to assist NYSLRS in meeting their internal control objectives, such as: the selection team for a QA vendor for the MEBEL Redesign Project; the adequacy of security requirements in the Redesign's RFP; and certain security requirements of the Backfile Conversion Project.*
- *OIA Operational Audit team audits of NYSLRS business units, which provide assurance regarding access controls for business users and the integrity of system data.*
- *Providing input to the OSC Information Security Office (ISO) Security policies and standards.*

In addition to Internal Audit coverage, NYSLRS IT audit coverage is also provided by:

- *Our independent external auditors (KPMG), who review the MEBEL system's IT general controls including review of the control environment, risk assessment process, information systems relevant to financial reporting and communication, and monitoring.*
- *A triennial independent Internal Control audit, which is required by the NYS Internal Control Act, and includes an evaluation and testing of the controls supporting programming and technical support for all system applications.*

OIA uses a risk based approach. The recommendation to establish an audit cycle for every element of an IT environment would not be practical. Currently, certain high-risk areas are periodically reviewed, such as infrastructure security and system access controls.

The Federal Financial Institution Examination Council (FFIEC) Handbook that you reference is not a set of standards that are applicable to Internal Auditing and OIA is not required to follow them. However, even this handbook discusses in detail that a risk-based approach is the most appropriate approach to increase audit efficiency and effectiveness. It states that "to determine the appropriate level of audit coverage for the organization's IT environment, management should define an effective risk assessment methodology." This handbook (which was updated in April 2012) recognizes the Institute for Internal Auditors (IIA) Standards by stating on page 9 "Institutions should consider conducting their internal audit activities in accordance with professional standards, such as the Standards for the Professional Practice of Internal Auditing issued by the Institute for Internal Auditors (IIA), and those issued by the Standards Board of the Information Systems Audit and Control Association (ISACA)."

As acknowledged by the FFIEC, the OIA is required to follow the Standards issued by the Institute of Internal Auditors (IIA). The IIA has published an IPPF Practice Guide in this regard: Global Technology Audit Guide #11 (GTAG #11) – "Developing the IT Audit Plan." In this guide, they quote from Brink's Modern Internal Auditing as follows:

"Auditors can use one of two strategies to arrive at the ideal frequency of planned audit activities:

- *The audit frequency is established in an initial risk assessment to take place every three to five years and is proportional to the risk level.*

- *The audit plan is based on a continuous risk assessment without a predefined audit frequency. Some organizations use this approach, which is especially appropriate within the context of the IT audit plan, given the higher rate of IT change as compared to changes in non-IT activities."*

OIA performs a comprehensive risk assessment process annually through which they obtain a great deal of information regarding processes and associated risks. They perform audits deemed the most critical or most beneficial based on an extensive risk assessment process. OIA and we agree that periodic coverage of data center security is necessary and audit coverage was provided in that area during your audit period. Another physical security review will be performed after the data center refurbishment project is completed.

The IT Audit team consists of an IT Audit Director and two IT Audit professionals. OIA agrees that additional staffing would allow them to provide broader audit coverage across the IT audit universe. OIA is working with our Office of Human Resources to identify qualified candidates.

[DFS Report]

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]

NYSLRS Response:

OSC follows the Civil Service requirements for hiring. There are requirements for the IT Internal Auditor titles, including college degrees and/or educational requirements and years of experience. A certification such as the CISA is deemed a plus, but not a requirement. OIA is not aware of any NYS IT internal auditing positions that require a certification either before or after hiring. Such a requirement would limit an already small field of potential qualified candidates, and would need to be established by the Department of Civil Service.

We strongly disagree with the inaccurate and inappropriate suggestion that the current members of our IT Audit Team are not highly qualified. The Director of the Team has 36 years of professional experience, which includes nearly 30 years of audit experience, 28 of which is in Internal Audit and 20 of which is in IT auditing. He has been the head of our IT Audit Team for nearly 20 years, is a Certified Information Systems Auditor (CISA), a Certified Internal Auditor (CIA) and a Certified Public Accountant (CPA). The two other IT auditors both have between 20 and 34 years of experience as either IT Professionals or IT Internal Auditors. One began her employment with OIA as an IT Auditor in 1997 with a very strong background in IT, application programming, system analysis, and IT project management (18 years). The second began her employment with OIA as an IT Auditor in 2002 with a similarly strong background in IT, application programming, systems programming, systems analysis, IT projects, and IT project management (10 years). This prior IT experience for both of them included some years working for the New York State Teachers' Retirement System (NYSTRS). During their years with OIA (each one now has over a decade of OIA IT auditing experience), they have displayed nothing but professionalism and dedication to OSC and NYSLRS. They have strong analytical and communication skills, a professional relationship with the Chief Information Officer's technical staff; know OSC's IT infrastructure, systems, and applications; and have provided valuable recommendations to management over the years. Overall, given their level of IT audit experience and knowledge of OSC's infrastructure, systems and applications, the IT team is extremely highly qualified to perform the IT Internal Audit work of the System. Also, in their memo dated August 9, 2012, the Department of Financial Services wrote that "IT audits are performed professionally by qualified auditors."

[DFS Report]

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]

14 Auditor Experience Summary Document.
15 *See* FFIEC IT Examination Handbook (August 2003), Audit Booklet, at pg. 11-12.

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.

NYSLRS Response:

OIA has developed a database for OIA's observations and recommendations that is intended to facilitate status reporting to higher management. OIA has always monitored follow-up status through use of their Audit Report database which indicates when the audit was issued, whether a follow-up audit is necessary, estimated date of follow-up, and the date the follow-up audit report is issued. The status of recommendations is monitored not only through the performance of formal follow-up audits, but through on-going communications with NYSLRS, the ISO, the Chief Information Officer, and the IT Governance committees. This is consistent with the IIA Standards, which require the "the chief audit executive must establish and maintain a system to monitor the disposition of results communicated to management." OIA has always had such a system. OIA performs follow-up audits for OIA audits that result in significant findings. The timing of follow-up audits is based upon consideration of the time needed by the client to remediate IT weaknesses and vulnerabilities. Sometimes the remediation is a time-consuming process; e.g., the procuring of additional security applications/systems, major changes to the IT business processes, and/or changes made through IT reorganization or reprioritizations. OIA does, however, communicate frequently with the Chief Information Officer and the ISO, as well as business units, to monitor the progress of remediation.

There is no evidence that any additional actions by OIA regarding outstanding issues would have quickened the IT remediation process. Management was aware of the major IT issues and directed attention to them. These key issues were always topics of discussion by NYSLRS management and OSC management as part of their strategic risk assessment process and the IT Governance process. In cases where critical IT issues identified by NYSLRS and OIA have not been remediated quickly, it was because those issues required long-term solutions. In our

experience, issues that can be immediately resolved by NYSLRS have been addressed quickly. However, many intrusion test findings required systemic changes to remediate, and were tracked by the ISO. One of the reasons that the audit "Follow-Up Review of Intrusion Testing of the Entire IT Infrastructure and the Portal Infrastructure (Audit #05-08)" was performed by OIA was to determine the level of remediation done for the OSC IT infrastructure prior to the implementation of the Statewide Financial System.

NYSLRS strongly disagrees with the statement that "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" is both inaccurate and irresponsible. There have been no serious IT failures at the NYSLRS. In fact, as noted in our response, our MEBEL system has a greater than 99% uptime.

IV. Conclusion [DFS Report]

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.

NYSLRS Response:

*OSC has an **Executive Policy on Responsibility for the Security of Information Technology Resources** to establish and maintain effective security over the hardware, software, programs and data associated with information technology (IT) installations. This policy lays out the structure and responsibilities of officials charged with developing security policies, standards, and guidelines for protecting the systems and the information they contain as well as establishing risk management processes for identifying, controlling, eliminating and/or minimizing events that can result in a loss of data or system resources.*

*The Retirement System routinely collects, maintains and distributes a variety of sensitive and/or restricted information. As a Division of the OSC, we adhere to the **Executive Policy on Use of and Access to Personal Information** which establishes general objectives with respect to the collection, use, access to, storage and disposal of personal information used in the course of our normal business activities. These policies are in place to protect the confidentiality and integrity of information in OSC's custody while maintaining the appropriate availability of that information for OSC's business purposes. The comprehensive agency-wide **Executive Policy on Responsibility for Information Security** guides OSC's information protection strategy in a continuously changing business and risk environment.*

Annually, the Deputy Comptroller for the Retirement Services, in the context of the Division's evaluation of their system of internal control, assesses the System's policies and practices for the use and safeguarding of personal information we possess and/or utilize during our normal business activities. Members of the Retirement Services Division's Senior Management Team are responsible for identifying their information security risks, mitigating and reducing those risks to acceptable levels, and reporting annually to the Deputy Comptroller, the Executive Deputy Comptroller and ultimately, the Comptroller on the status of their risks through the Internal Control Certification process.

Incidents involving the disclosure of personal or private information to unauthorized individuals are covered under the agency's ***Policies and Procedures Notification Procedure for Security Breaches Involving Personal and Private Information****. The Comptroller expanded the notification requirements of the Information Security Breach and Notification Act (Chapters 442 and 491 of the Laws of 2005) to include the disclosure of non-electronically maintained information. Given the volume of correspondence handled by the System, the overwhelming majority of incidents involve human error, such as the double insertion of letters. Jack McPadden serves as the System's Privacy Liaison and incidents are brought to his attention. Utilizing the course of action determined by the policies and procedures, he works with the agency's Privacy Officer and the Deputy Comptroller to provide notification to affected individuals.*

[DFS Report]

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.

NYSLRS Response:

We have always employed proactive efforts and continued vigilance to protect the system's information technology against emerging risks. As a matter of fact, we believe OSC/NYSLRS to be a recognized leader in having adopted policies covering IT governance, risk management and internal controls. Additionally, as referenced in this report and response, we have an Information Security Officer, an IT internal audit unit, and we conduct IT assessments, penetration testing and disaster recovery testing. As our response clearly indicates, there are written policies covering access and use of sensitive information, and specific offices and

individuals charged with ensuring that those policies are adhered to and updated as necessary to reflect ever changing technological advances. In summation, we believe that the existing system of internal controls adopted for the agency, and adhered to by the Retirement System, not only meets, but would exceed anything required under an industry-wide standard.
