STATE OF NEW JERSEY
OFFICE OF THE STATE COMPTROLLER

DEPARTMENT OF THE TREASURY

DIVISION OF PURCHASE AND PROPERTY

AND

DIVISION OF PROPERTY MANAGEMENT AND CONSTRUCTION

DISPOSITION OF EXCESS AND SURPLUS COMPUTER EQUIPMENT

A. Matthew Boxer
COMPTROLLER

March 9, 2011
PA-12

TABLE OF CONTENTS

BACKGROUND

To achieve the maximum possible benefit from computer equipment, the State's Department of the Treasury (Treasury), Division of Purchase and Property (DPP), requires that all excess computer equipment in the possession of a State agency be made available to other State agencies. Computer equipment is considered excess when an agency, at its discretion, determines the equipment no longer meets the agency's operational needs.

Treasury's Circular Letter 00-17-DPP sets forth specific policies and procedures concerning the redistribution of such excess equipment to State agencies. According to the Circular Letter, prior to sending excess equipment for redistribution, State agencies are required to remove all data from the computer's hard drive. The agency is then required to separate the equipment into two categories, working and non-working, and notify the Surplus Property Unit within DPP that the equipment has been declared excess.

Upon receipt of that notification, the Surplus Property Unit is required to notify all other State agencies of the availability of the equipment. If the equipment is not claimed by another agency within 30 calendar days, the equipment is to be declared as surplus and disposed of through either sale or donation. In that regard, DPP manages public auction sales as well as a program to donate computers to local governments and non-profit organizations. The redistribution itself is performed by staff from Treasury's Division of Property Management and Construction (DPMC), specifically, staff from DPMC's Bureau of Special Services' warehouse (Warehouse).

From January 2009 to March 2010, the Warehouse redistributed for reuse to State agencies a total of 2,357 desktop computers, laptop computers, hubs and servers that otherwise would have been removed from operation. The

Warehouse also receives and redistributes other State equipment, such as furniture, which was not the subject of this audit.

In early 2007, allegations arose that Warehouse employees had been engaged in various illegal activities concerning surplus property in the Warehouse. These activities included, among others, stealing surplus metal equipment and selling it as scrap, and rigging auctions for surplus computer equipment. As a result of an investigation conducted by the New Jersey State Police and the State's Division of Criminal Justice, the Warehouse's five employees were charged with various theft-related and official misconduct offenses. Four have since pled guilty. Charges are still pending against the fifth employee. As a result of these events, four of the Warehouse employees were terminated and the fifth is on a disciplinary suspension, resulting in the turnover of the entire Warehouse staff. The turnover of the Warehouse staff, and the problems that led to that turnover, contributed to the decision to engage this audit.

AUDIT OBJECTIVE, SCOPE AND METHODOLOGY

The objective of our audit was to assess the adequacy of the State's internal controls over the process of redistributing excess computer equipment and disposing of surplus computer equipment, including protecting any sensitive or confidential information contained therein. Our audit covered the period from July 1, 2008 to December 16, 2010.

This audit was performed in accordance with the State Comptroller's authority as set forth in *N.J.S.A.* 52:15C-1 et seq. We conducted our audit in accordance with generally accepted government auditing standards applicable to performance audits. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

To accomplish our objective, we reviewed relevant statutory laws, administrative code provisions, circular letters, departmental policies and procedures, and industry standards, such as the Control Objectives for Information Technology issued by the Information System Audit and Control Foundation. Compliance with those provisions that we considered significant was determined through interviews, observations and tests of sampled transactions. In addition to reviewing processes used by Treasury, we reviewed processes used at four State agencies that sent the surplus items for disposition.

We limited our testing of equipment to personal desktop computers, laptop computers and smart phone communication devices. Due to the absence of a written inventory of equipment in the Warehouse at the time of our sample selections, we used a non-statistical sampling approach.

Concerning smart phone devices, of the 15 devices we obtained, only one contained data. This device showed the name of the former user and the presence of messages, but was locked by a password. We did not take steps to bypass this security feature.

During the course of our audit, we also became aware of a potential violation of law by a Warehouse staff person. Due to the nature of this issue, we are not including it in our report. Instead, we referred this matter to the Division of Criminal Justice for review.

SUMMARY OF AUDIT RESULTS

Our audit found that multiple State agencies were not complying with the State's requirements concerning the disposition of excess and surplus computer equipment. For example:

- State agencies disposed of computer equipment without ensuring that data on the devices had been properly removed. Data we found on such devices was of a personal and confidential nature, including: completed tax returns; Social Security numbers; names, addresses and phone numbers of children placed outside of the parental home; a list of State computer sign-on passwords; and child abuse documentation including the names and addresses of the children. Many of these items were found on computers packaged for public auction. In total, we found data on 46 of the 58 hard drives we tested (79 percent).

- Contrary to State requirements, agencies sent to the Warehouse shipments of computer equipment with no packing lists, no indication of the equipment's working order and no certification that the equipment's data had been removed. The shipments were accepted by the Warehouse.

- More than 100 computers and more than 900 cellular telephones were redistributed to particular local governments and non-profits without following the requirements of State law to provide equal access to and broad notice concerning the availability of such equipment. For example, the cellular telephones were set aside specifically for a particular non-profit. This practice also violated the requirement that State agencies be afforded the right of first refusal concerning such equipment.

We make ten recommendations to address the deficiencies we identified.

AUDIT FINDINGS AND RECOMMENDATIONS

Data Security

State agencies are disposing of computer equipment without ensuring that data has been properly removed.

Treasury's Circular Letter 00-17-DPP requires that all computer hard drives be "degaussed" by the sending agency and the operating system be reinstalled prior to delivery to the Warehouse. Degaussing is the process of exposing media, including computer hard drives, to a strong magnetic field to purge the electronic data contained therein. The purging of data is designed to prevent the unauthorized disclosure of confidential information in violation of federal and State law.

As part of our audit research process, in January 2010 we obtained six hard drives and one laptop computer from the Warehouse. Despite the State's degaussing requirements, one of the hard drives contained a list of children placed outside the parental home, and the laptop contained numerous files of a State judge, including:

- the judge's life insurance trust agreement, his tax returns for three years and a final mortgage payment letter that included the address of the property and the account number;
- two documents with the judge's Social Security number;
- a "confidential fax" to the New Jersey Lawyers Assistance Program concerning an attorney's "personal emotional problems"; and
- non-public memoranda by the judge concerning potential impropriety by two attorneys.

As part of our audit, we visited the Warehouse on three additional occasions during February and March 2010. We examined a total of 103 computers and found 39 with hard drives. As pictured below, some of these computers were shrink-wrapped on pallets ready for sale at public auction.

We noted that four of the 103 computers were still under the vendor's warranty, yet the four computers were packaged to be sold at auction as scrap. Through service tags on the computers, we determined the agency that sent these four computers to the Warehouse. Personnel from that agency stated that the computers had been transferred to the Warehouse in error.

We also obtained from the Warehouse 19 other hard drives which previously had been removed from computers, for a total of 58 drives. To determine what information, if any, was on the 58 hard drives, we connected each to a personal computer. If the data was not immediately viewable, we scanned the drive with an inexpensive, off-the-shelf software program designed to retrieve deleted data, which is available for retail purchase.

We categorized the data files on the 58 hard drives using security classifications promulgated by the State's Office of Information Technology (OIT) and set forth in Treasury's Circular Letter 08-04-S1-NJOIT. Those classifications and

their definitions, starting with the classification for the most highly protected information are:

- *Personal* – Personally identifiable information pertaining to individuals that is protected by federal or State law.

- *Confidential* – Information of a sensitive nature that is available only to designated personnel.

- *Secure* – Information that is available to agencies and used for official purposes but would not be released to the public unless requested.

- *Public* – Information that is authorized for release to the public.

For our testing purposes, we also used two additional classifications: "nonbusiness" and "no data." We used the "nonbusiness" classification where the information found on the drive was unrelated to State business, such as the user's resume. We used the "no data" classification where no data was found or recoverable during testing of the drive.

Despite the State's degaussing requirements, we found data on 46 of the 58 hard drives (79 percent). Of those 46 hard drives, we found business-related data on 37 of them. The remaining 9 drives contained only nonbusiness-related data.

The business-related data we identified included proprietary software and a list of State-supervised children, along with their dates of birth and Medicaid numbers. Social Security numbers for either State employees or members of the public were found on six drives. A summary of the data we found on the drives by level of classification is shown in Table 1 below. We classified the hard drives based on the most highly protected category found on a drive.

Table 1: Business-Related Data Found on Hard Drives

Highest Data Classification Found on Drive	Number of Drives Where Such Data Was Found
Personal	13
Confidential	5
Secure	14
Public	5
Total	37

We noted that 13 of the 37 drives containing business-related data were packaged for public auction at the time of our review. We selected 5 of those 13 drives for a more detailed review. Our examination revealed that those five drives contained:

- More than 230 files related to State investigative case screenings and reports of child abuse, endangerment and neglect. Many of the reports contained the names and addresses of the children. The files also included a child fatality report, child immunization records and a child health evaluation.

- Information identifying the user of the hard drive as a high-level State agency official, internal agency memoranda, internal written briefings for an agency Commissioner, draft documents, personal contact information for multiple members of the then-Governor's cabinet, and work plans for individual staff members.

- A list of vendor payments referencing names of children and names, addresses and phone numbers of children placed outside of the parental home, along with case information.

- A Microsoft Outlook e-mail archive containing 46 e-mails, including one listing multiple users' computer sign-on passwords, as well as

personnel reviews for State employees that included their Social Security numbers.

The availability of such confidential personal information and sensitive business information to third parties through the disposal of State-owned computer equipment presents security risks to the affected individuals and State agencies. Further, the release of such information to unauthorized parties would violate various federal and State statutes.

During the course of our audit, DPMC and DPP informed us that they previously became aware in 2009 of similar instances in which computer equipment was sent to the Warehouse containing data. DPMC and DPP reported that the two agencies involved were reminded at that time of their obligation to remove data from computer equipment prior to sending it to the Warehouse. Nonetheless, one of those agencies was among the four agencies our audit found in 2010 sending equipment to the Warehouse containing data.

As part of our audit, we met with the four State agencies whose data we identified to inform them of our findings and discuss their computer disposal processes. Two of those agencies informed us that they did not have degaussing equipment available to them, but all of the agencies were able to identify some process they had in place for data removal. In response to our findings, the agencies cited steps they would take to prevent future disclosure of confidential data. For example:

- One agency confirmed having degaussing equipment available, but stated that staff was reluctant to use it because of the noise and magnetic fields it generated. This agency's corrective actions included issuing a new policy governing information disposal and media sanitation, and developing new procedures for sending surplus computer equipment to the Warehouse. The agency's new policy directs that if the hard drive is not functional or cannot be wiped clean, it is to be destroyed.

- Another agency said that the person likely responsible for having provided the equipment to the Warehouse without removing its data was no longer employed by the agency. In addition, the agency provided us with a series of corrective actions it would undertake, including steps to increase control over its data removal process. The agency indicated it also will conduct periodic audits of equipment identified for disposal to ensure that all data has been completely removed.

We separately note that compliance with the particular data purging process detailed in Circular Letter 00-17-DPP may not be possible if other surplus program goals are to be met. Specifically, the Circular Letter requires that a degaussing procedure be used to purge data. However, degaussing usually destroys the hard drive and prevents the reinstallation of an operating system since the software that manages the drive is also destroyed. To continue the State's redistribution program in a fully effective manner, a non-destructive solution, such as a software-based means of purging data, would need to be implemented.

After we informed DPP of our audit findings, DPP temporarily suspended auction sales. DPP also informed State agencies of the data issues we identified. Modified policies and procedures designed to comply with OIT data protection policies and increase overall data security followed. On September 24, 2010, DPP sent an e-mail to all State agencies stating that as an interim measure, the Warehouse will no longer accept storage media, including computer hard drives, and that disposing of (and sanitizing) data storage devices will be the sole responsibility of the owning agency.

At the audit exit conference, DPP informed us that they were taking additional steps to help agencies protect their data. For example, DPP is currently exploring alternate means of preventing data loss from hard drives. DPMC

stated that they now require all agencies sending computer equipment for sale to certify that the hard drives have been removed.

Recommendations

1. Enforce compliance with Circular Letter 00-17-DPP to ensure that all data is removed from State computer equipment before being sold to the public or donated.

2. In consultation with OIT, determine a data removal method that satisfies the State's data security requirements while minimizing any diminution in the value of the equipment.

3. Ensure that equipment still under warranty is not sold at auction as scrap.

Computer Equipment Controls

Internal Controls over excess and surplus equipment are not sufficient.

As part of our audit we also reviewed the State's internal controls related to excess and surplus computer equipment. As noted previously, Circular Letter 00-17-DPP outlines the process to be used for the disposition of such computer equipment, including detailed steps to be performed by the sending agency. While not named in this Circular, DPMC functionally executes much of this process. Excess equipment is to be offered to other State agencies and, after a period of time, sent for disposition through sale or donation. Agencies are required to supply to the Warehouse detailed documentation about such equipment, including a detailed packing list and a description of its functional status (e.g., working, non-working), as well as a certification of data removal.

Our testing revealed that this required process is not being followed. Specifically, we reviewed documentation for 11 computer-equipment shipments to the Warehouse over a two-week period in March 2010. Of the 11 shipments, 2 did not have a detailed packing list or similar inventory. None of the 11 included a certification that data had been removed from the equipment and none had any indication of the working status of the equipment. Among other consequences, those deficiencies compromise controls concerning theft prevention and detection, as there is no record of what equipment should be available at any given time.

During this same time period, we also observed two additional shipments of computers being received at the Warehouse. Warehouse staff did not reconcile the equipment received with a packing list in the one instance when such a list was available. In the other instance, contrary to the requirements of the Circular Letter, there was no packing list, but the shipment was accepted anyway.

Moreover, the process being used by DPMC staff to redistribute the computer equipment does not comply with Circular Letter 00-17-DPP. For example, that Circular Letter requires that the Warehouse notify all other State agencies of the availability of any surplus equipment. Agencies can also request such equipment through an e-mail clearinghouse. Warehouse staff told us that they follow this procedure. However, when we requested the State agency contact list used by Warehouse personnel, none was available. Then, when one was created solely to address our request, it consisted simply of a compilation of individuals who in the past had removed computer equipment from the Warehouse. Not every State agency was included on the list.

We also observed that Warehouse staff rely on their own understanding concerning individual equipment needs, thereby circumventing the State's prescribed redistribution process. For example, we observed on one occasion Warehouse staff offering computer equipment by cellular telephone to an individual from a State agency as it was being unloaded into the Warehouse. When we contacted the receiving agency's Information Technology staff, they were not aware of any equipment being acquired by this individual for reuse at the agency. Failing to follow required distribution processes can result in equipment being redistributed in an inefficient, unlawful or unfair manner.

To control access to the Warehouse, visitors and individuals picking up equipment are required to sign in and sign out. However, when we reviewed the sign-in sheet to obtain information concerning the individual who picked up the equipment referenced in the previous paragraph, his name was not listed on the sheet. When we questioned the individual, he stated that he was aware of the sign-in sheet, but did not always sign in when he went to the Warehouse.

It appears that at times certain State agency staff receive preferential treatment with regard to obtaining computer equipment from the Warehouse. According to one Warehouse employee, he is sometimes asked by agency staff if he needs anything to make his job easier, such as office supplies or office equipment. On

one occasion, the employee obtained from one such staff person six boxes of copier paper, four flash drives, four boxes of pencils, and pens. The agency staff person, in turn, was provided with selected pieces of computer equipment.

We found similar problems in procedures being used for equipment donations to local governments and non-profits. Pursuant to *N.J.A.C.* 17:12-9.4, such donations are to be made quarterly and only after State agencies have been notified of the computer equipment available. That regulation further states that information about available computer equipment should be "announced through a dedicated telephone line" and posted on the internet for potential recipients. However, we found that since 2008 the donation program has not been administered as prescribed. For example, we observed select local government representatives in the Warehouse picking up equipment without other local governments and non-profits having received equal access to or notice of that equipment. We further found that the Warehouse, in some instances, violates the requirement that State agencies be given first access to such equipment.

In total, our review of redistribution logs covering a 15-month period (January 2009 to March 2010) found that more than 100 computers and more than 900 cellular telephones were redistributed to local governments and non-profits in violation of the requirements of the donation program. For example, during the 15-month period, all 900-plus cellular phones were set aside for one particular non-profit, which was directly contacted by Warehouse personnel as the phones became available. The Warehouse staff had been referred to the non-profit by another State agency.

In our review of controls at the Warehouse, we further noted that much of the computer equipment disposition process and related controls at the Warehouse are executed by a single individual. Although participants from a career training program operated by the State's Juvenile Justice Commission assist in these processes, this one individual reviews equipment upon arrival for usefulness, tests it, rebuilds it and disposes of it through redistribution to

agencies, donation or auction. Risks involving theft or other improprieties are increased when a process such as this one is controlled by one person. Such single-handed control also can result in inefficiencies, such as in the event of the individual's extended absence. DPMC management conceded that without the efforts of this individual, the State's processing of computer equipment for redistribution would cease.

Lastly, we noted that neither DPP nor DPMC have conducted a complete accounting of the financial benefits associated with the computer equipment redistribution program. Greater fiscal accountability would aid in determining whether the resources and internal controls used to manage the redistribution process are appropriate and what the ultimate value of the program actually is.

Recommendations

4. Require agencies to notify the Warehouse when they intend to send a shipment of equipment to the Warehouse, and to include with any shipment a detailed packing list, a certification of data removal and a description of the functional status of the equipment. Monitor compliance with these requirements.

5. Develop and maintain an appropriate system of control over equipment and periodically conduct reviews to ensure that it is operating as intended.

6. Develop a reliable contact list for all State agencies and follow a standard contact process to ensure that the maximum benefit from surplus equipment is realized by the State.

7. Ensure that equipment is provided to local governments and non-profits only through the prescribed donation program.

8. Evaluate and allocate the appropriate resources to the Warehouse to meet the goals of the surplus program and provide adequate controls.

9. Develop a system to track the financial benefits of the computer redistribution program.

10. Determine appropriate processes concerning excess and surplus computer equipment and update policies, procedures and Circular Letters accordingly. Monitor adherence thereto.

REPORTING REQUIREMENTS

We provided a draft copy of this report to Treasury officials for their review and comment. Their comments were considered in preparing our final report and are attached as Appendix A.

Treasury's response pointed out that by our staff keeping Treasury apprised of our findings as the audit progressed, it was able to expeditiously address those issues. To that end, the response includes a series of steps Treasury took during the course of the audit to prevent future release of personal and confidential data from surplus computers destined for auction. The response also includes a series of additional steps either underway or under consideration to address our recommendations.

The Office of the State Comptroller is required by statute to monitor the implementation of our recommendations. To meet this requirement and in accordance with *N.J.A.C.* 17:44-2.8(a), following the distribution of the final audit report, Treasury shall report to the Office of the State Comptroller within 90 days stating the corrective action taken or underway to implement the recommendations contained in the report and, if not implemented, the reason therefore.

State of New Jersey
DEPARTMENT OF THE TREASURY
DIVISION OF PURCHASE AND PROPERTY
OFFICE OF THE DIRECTOR
P. O. BOX 039
Trenton, New Jersey 08625-0039
TELEPHONE (609) 292-4886 / FACSIMILE (609) 984-2575

CHRIS CHRISTIE
Governor

KIM GUADAGNO
Lt. Governor

ANDREW P. SIDAMON-ERISTOFF
State Treasurer

Location:
33 W. STATE STREET
TRENTON, NJ

February 17, 2011

Mr. A. Matthew Boxer
State Comptroller
Office of the State Comptroller
P.O. 024
Trenton, NJ 08625-0024

Dear Mr. Boxer:

Thank you for providing the Department of the Treasury an opportunity to respond to your audit of the Division of Purchase and Property (DPP) and the Division of Property Management and Construction (DPMC) regarding the disposition of surplus computer equipment, and for keeping Treasury apprised of your findings as the audit progressed. This has permitted Treasury to expeditiously address issues identified in the audit. Our response to each of the audit recommendations is below, but we would first like to outline the actions already taken to address these issues.

Since our July 12, 2010 meeting, when your Office disclosed that personal and confidential data was found on surplus computers destined for auction, Treasury has taken the following actions:

- DPP immediately suspended all auctions of surplus computers. All data storage devices have been removed from these computers and the CPUs were subsequently auctioned without storage devices.
- DPMC immediately notified their surplus contacts that all movement of surplus computer equipment containing data storage devices was suspended. DPP sent formal notice of this change to all agency IT Directors.
- On September 24, 2010, DPP published an interim policy for handling surplus computers that requires the using agencies to remove all storage devices and hold them pending further direction on proper data cleansing or destruction.

Treasury is currently developing a permanent policy for handling surplus computers and the Office of Information Technology (OIT) is examining whether revisions to its data security policies are warranted. When these efforts are complete, new procedures will be memorialized in a revised Circular Letter governing the disposition of excess and surplus computers.

Audit Recommendations and Responses

1. Enforce compliance with Circular Letter 00-17-DPP to ensure that all data is removed from State computer hard drives before being sold to the public or donated.

   We concur with the intent of this recommendation, but must point out that the agencies who own data must continue to bear the ultimate responsibility for the security of that data and for cleansing data storage media according to the security classification of the data it contains. These responsibilities are set-out in OIT Policy 09-10-NJOIT, "Information Disposal and Media Sanitization." Treasury has neither the resources nor the expertise to check all storage devices for data, or to enforce compliance with the OIT policy. More importantly, the OIT policy clearly states that agencies are accountable for the classification of their data and that security measures must be commensurate with the type/sensitivity of the data being collected and stored. Since Treasury does not "own" the data, it is not in a position to judge whether or what level of data removal might be appropriate for any given drive. These decisions must be made by the data-owning agencies.

   Treasury has therefore concluded that the only way to ensure that no data leaves State control is to ensure that no data storage device leaves State control, which is the gist of the interim policy. Revisions to this policy are under consideration, and OIT is currently examining whether revisions to its data security policies are warranted. As noted above, when these efforts are complete, new procedures will be memorialized in a revised Circular Letter.

2. In consultation with OIT, determine a data removal method that satisfies the State's data security requirements while minimizing any diminution in the value of the equipment.

   OIT is currently examining whether revisions to its data security policies are warranted and what, if any data removal method can be relied upon to ensure protection of sensitive data. Unless and until OIT certifies such a method, Treasury will continue to require the removal and destruction of all data storage devices prior to accepting possession of, transferring, or disposing of all computer equipment. Treasury has concluded that the diminution of value is of minor consequence compared to the potential harm that could ensue from the inadvertent release of personal and confidential data.

3. Ensure that equipment still under warranty is not sold as scrap.

   We concur that equipment under warranty should not be declared excess or surplus, but Treasury must defer to the owning agencies to address this issue. Since the equipment was procured by the using agencies, only they have the ability to assess whether a piece of equipment has outlived the warranty provisions.

4. Require agencies to notify the Warehouse when they intend to send a shipment of equipment to the Warehouse, and to include with any shipment a detailed packing list, a certification of data removal and a description of the functional status of the equipment. Monitor compliance with these requirements.

   Under the September 24th interim policy, a packing list and certification of data storage device removal are required for all equipment containing data storage devices and all such shipments must be preapproved and scheduled in advance. This requirement will continue. These procedures are not required for monitors, keyboards, printers, or other equipment without data

storage capability, as this would impose a large administrative burden while providing little benefit. Similarly, the requirement to describe the functional status of surplus equipment is not currently enforced because this would impose an administrative burden on the Agencies, the cost of which would exceed the value of the assets. These requirements will be removed from the Circular Letter.

DPMC is currently holding a sample of CPUs surplussed under the interim procedures for a possible compliance audit, but Treasury does not have the resources (auditors) to conduct that audit. We would invite the Comptroller's Office to assist us by providing this resource as a follow-up to this audit.

5. Develop and maintain an appropriate system of control over equipment and periodically conduct reviews to ensure that it is operating as intended.

   A comprehensive inventory control system to track surplus assets is neither warranted nor cost-effective, given the minimal value of these assets. However, we agree that improved controls over facility access and the movement of surplus assets at the 1st Avenue warehouse will minimize the potential for theft or misappropriation. To that end, DPMC will employ and enforce employee and visitor sign-in procedures, improve supervision of loading and unloading operations, and require escorts for visitors. These measures are now in place. Other deterrence measures such as cameras and security guard are also currently in place.

6. Develop a reliable contact list for all State agencies and follow a standard contact process to ensure that the maximum benefit from surplus equipment is realized by the State.

   We concur. Treasury has compiled a list of Agency IT Directors and other IT contacts for this purpose. Redistribution of computers is currently suspended pending a final determination of how to protect data security. Should we resume the redistribution program, a standard contact process based upon this list will be used.

7. Ensure that equipment is provided to local governments and non-profits only through the prescribed donation program.

   We concur. No offer of surplus State computers will be made outside of the prescribed donation program. We would also note that the Surplus Computer Donation Program is currently suspended pending a final determination of how to protect data security.

8. Evaluate and allocate the appropriate resources to the Warehouse to meet the goals of the surplus program and provide adequate controls.

   We agree in principle, but must note that personnel assigned to the 1st Avenue warehouse are involved in other areas besides the surplus computer program. Treasury considers data security to be of high priority but we must recognize that there are scarce manpower resources within the State.

9. Develop a system to track the financial benefits of the computer redistribution program.

If Treasury determines that data security can be ensured, and redistributing computers continues to make economic sense, financial benefits of the program will be tracked.

10. Develop appropriate processes concerning excess and surplus computer equipment and update policies, procedures and Circular Letters accordingly. Monitor adherence thereto.

    We concur. As outlined above, those efforts are underway, and we will update you as to their progress.

Sincerely,

Lignasa Desai-McCleary
Acting Director
Division of Purchase and Property

Steven Sutkin
Director
Division of Property Management and Construction