In the matter of the
Complaints Commissioner Law (2006 Revision)

Own Motion Investigation

The Appropriate Disposal of Electronic Data Storage Containers (EDSCs)

Own Motion Investigation Report Number 13

Prepared by the Office of the Complaints Commissioner

Date: 7 April 2009

Published under the Authority of the Office of the Complaints Commissioner

PO Box 2252
208 Piccadilly Centre
28 Elgin Avenue
Grand Cayman
KY1-1107
Telephone (345) 943-2220
Facsimile (345) 943-2221

Aim of the Office: To investigate in a fair and independent manner complaints against government to ascertain whether injustice has been caused by improper, unreasonable or inadequate government administrative conduct, and to ascertain the inequitable or unreasonable nature or operation of any enactment or rule of law.

TABLE OF CONTENTS

	SECTION	PAGE
1.	Foreword	5
2.	Executive summary	5
2.1	Scope of investigation	5
2.2	Record of ministries	6
2.3	Evidence from individual COs	7
2.4	Findings from the CSD	8
2.5	Key findings	9
2.6	Analysis	10
2.7	Conclusion	11
2.8	Recommendations	12
3.	Introduction	12
4.	Background	14
5.	Purpose of investigation	18
6.	Method	19
7.	Findings	20
7.1	Cabinet Office	20
7.2	Portfolio of Internal and External Affairs	21
7.3	Portfolio of Finance and Economics	22
7.4	Portfolio of the Civil Service	24
7.5	Ministry of Health and Human Services	25
7.6	Ministry of Education	26
7.7	Ministry of District Administration, Planning, Agriculture and Housing	27
7.8	Ministry of Communications, Works and Infrastructure	27
7.9	Ministry of Tourism, Environment, Investment and Commerce	28
7.10	Summary of findings from Portfolios and Ministries	29
7.11	Findings from the CSD	30
7.11.1	Records	30
7.11.2	Quality of service	31
7.11.3	External controls	32
7.11.4	Internal controls	33
7.11.5	Classification of data	33
7.11.6	Clarity of service requested and provided	34
8.	Overall summary of findings	35
9.	Analysis	36
10.	Conclusion	37
11.	Recommendations	39

1. Foreword

Analyst Scott Swing completed this report, in accordance with the powers conferred on the Commissioner under Section 6 of the Complaints Commissioner Law (2006 Revision).

2. Executive Summary

2.1 Scope of investigation

Technological advances have made it possible for information to be stored electronically by an ever-growing number of devices. Sometimes, little thought is given to the type of information being collected, while it is often the case that few users have an understanding as to what information remains on the device when it has reached its functional life limit and is set out for disposal.

This report focuses on the disposal of electronic data storage containers ("EDSCs"). This class of device includes computer hard drives and memory chips in photocopiers, scanners, cameras, fax machines, cell phones and personal digital assistants (PDAs) including Blackberries. EDSCs also include floppy disks, diskettes, CDs, DVDs, USB thumb drives/jump drives, audio and videotapes and smart cards. It must be noted that USB jump drives are almost certainly all capable of storing more information than a civil servant would typically produce in a year.

Failure to properly dispose of EDSCs could result in the unauthorized release of personal information gathered by government (including medical records and personal financial information), as well as sensitive information about the operation of government, to persons who could use this information for improper purposes.

The Office of the Complaints Commissioner ("OCC") conducted some preliminary inquiries that led to the conclusion that there was cause for concern about how EDSCs were being handled and ultimately disposed of by government. The Commissioner determined that it was in the public interest to launch an own motion investigation to determine whether government was properly disposing of EDSCs when they were no longer of use to government.

The Commissioner decided that this investigation should be directed towards the Chief Officers ("COs") of the following entities: Cabinet Office; Portfolio of the Civil Service; Portfolio of Internal and External Affairs; Portfolio of Finance and Economics; Ministry of Education, Training, Employment, Youth, Sports and Culture; Ministry of Tourism, Environment, Investment and Commerce; Ministry of District Administration, Planning, Agriculture and Housing; Ministry of Communications, Works and Infrastructure; and the

The Ministries and Portfolios had also not dealt with the question of information transferred from work being left on civil servants' home computers.

2.3 Evidence from individual COs

Several of the COs interviewed during the OCC's investigation made revealing statements.

The CO of the Portfolio of Internal and External Affairs, Mr. Donovan Ebanks, stated that the issues raised by the OCC's investigation had focused due attention on the issue. He admitted that there was a need to revisit the Portfolio's practices, including a review of the SLAs with the CSD for the coming financial year, saying that he felt that the proper disposal of EDSCs needed to be specifically addressed within the SLAs. He also revealed that a number of computers from his Portfolio had at one time been donated to the prison's educational program (and could not be verified as having been wiped).

Echoing CO Mr. Donovan Ebanks, the CO for the Ministry of Health and Human Services, Mrs. Diane Montoya, also stated that the investigation had been helpful to her Ministry, as it had highlighted many of the issues that it needed to consider regarding the secure use and disposal of EDSCs. She admitted that she had never even considered the disposal practices for many of the EDSCs that were listed in the OCC's opening letters to the COs. She also confirmed that she did not know what happened to the equipment once it was entrusted to the CSD for disposal.

The acting CO of the Ministry of District Administration, Planning, Agriculture and Housing, Ms. Jennifer Ahearn, in acknowledging that EDSCs needed to be better tracked to ensure that they were properly secured during use as well as properly disposed of, proposed that government might develop a "centralized, uniform, prescriptive policy specific to the disposal of EDSCs".

The potential problems raised by secure remote access to government information were highlighted by the CO for the Ministry of Tourism, Environment, Investment and Commerce, Ms. Gloria McField-Nixon. She stated that officers with Citrix tokens would occasionally use internet cafes and hotel business centres to access the Ministry's network while away from the Cayman Islands, although only if they were on personal leave and needed to respond to an urgent matter – otherwise, they would respond from their government-issued laptop computer.

On the matter of Blackberries, she stated that her own device had the ability to edit documents and send them back to other users. As someone who travelled regularly with her job, she noted that remote access had become a

put in other computers within government. He testified that once a hard drive was no longer of use to government, the CSD would take it to the landfill and destroy it with a sledgehammer. He added that the CSD did not remove the platter from the casing but simply smashed up the whole case.

2.5 Key findings

1. None of the Portfolios and Ministries investigated had a policy for addressing the disposal of EDSCs. It was also determined that none of the Ministries and Portfolios had sufficient procedures to demonstrate that they were properly managing and disposing of EDSCs.

2. With the exception of the Department of Tourism under the Ministry of Tourism and the Department of Education under the Ministry of Education, which had their own internal IT support functions for limited areas, all the Ministries and Portfolios claimed that they and their respective departments relied on the CSD to provide for the disposal of IT equipment including Blackberries when and if the need arose.

3. There was an overall lack of adequate documentation of EDSC disposal throughout the Ministries and Portfolios as well as at the CSD.

4. There was a general lack of awareness on the part of COs as to what should be done with EDSCs, as well as what was ultimately being done with EDSCs. Most of them were aware of their procedure for removing the actual asset from their asset registry, but once that process was completed there was no corporate memory and no further paper trail that could sufficiently verify what had happened to the EDSCs.

5. Until the launch of this investigation, the CSD would provide disposal services to any government department that requested this service. Once the computer had been properly removed from an entity's asset registry, the CSD would assess whether any parts could be salvaged for spare parts. This process included saving the hard drives if they could be used in other machines. These hard drives, if kept, were re-imaged. They would only be wiped if that process had been specifically requested by the entity. Once the computer had been stripped of any useful parts, the CSD would then take the remaining equipment to the landfill. While the CSD indicated that these machines were crushed, there was no way to verify if in fact that was being done. In the past, the CSD would only use a sledgehammer to smash hard drives deemed to be of no useful purpose.

6. It was apparent that communication between departments and CSD was not precise and that terminology was not used consistently. This may have resulted in a particular department seeking a higher level of service than was actually provided by the CSD.

The creation and implementation of a data classification system remains a project that should be completed. The failure to classify data and the resulting inability to know the level of care to be taken in decommissioning an EDSC impairs the design of an efficient and cost effective recycling and disposal process.

The use of personal computers and their retention of government information was an issue that was beyond the technical expertise of many of the COs interviewed. It is appropriate, then, to emphasize the need for this issue to be addressed while policy is developed. While it is true that the data transferred to a personal computer is still owned by government, and covered by confidentiality undertakings provided by government employees, arrangements must still be made for its proper disposal.

2.7 Conclusion

This own motion investigation by the OCC found that COs were not adequately tracking the use and disposal of EDSCs within their respective Ministries/Portfolios. Until the launch of this investigation by the OCC, very little attention had been given to the issue of secure disposal of EDSCs. It was clear that COs were unaware of what was being done with the EDSCs being disposed of from their Ministries/Portfolios and the departments under them.

While it has also become clear that not all EDSCs pose significant risk to the security of sensitive information, there is no way of clearly identifying which ones could pose a serious risk as information has not been classified. Regardless of what EDSCs are being considered, and regardless of what information is being stored on these containers, the process of tracking and monitoring the disposal of these containers has been insufficient to ensure that EDSCs are being disposed of properly.

As the COs have the responsibility of overseeing the assets of their Portfolio/Ministry as well as ensuring that records are being securely maintained, each Portfolio/Ministry must have a policy that provides for the secure maintenance and disposal of all EDSCs. However, the policy required for such a process need not be specifically designed to be unique to each Portfolio/Ministry and it is likely best that there be one policy developed for all of the public sector. The expertise required for the development of the policy potentially could come from the CSD, CINA and existing published works from abroad. It would be appropriate for the Chief Secretary to take oversight of this project. However, no objection would be raised if the issues were addressed as part of the current process to amend the Financial Regulations under the direction of the Financial Secretary.

What is a proper policy for the disposal of EDSCs? The new policy and procedures must protect private and sensitive information to a degree that is

The practices of many government entities regarding the secure disposal of EDSCs appeared not to be in accordance with reasonable disposal practices. For example, the OCC received testimony from a local charity that had been donated several used computers by a government entity that deals with highly sensitive information. As a matter of routine, the charity checked the computers to ensure they were in good order prior to putting them into service. During this check, the charity discovered that the government entity had not removed all government information from the computers. While the charity administrator did not open individual files, its testimony leads to the conclusion that many files, including some which may have contained very sensitive personal information, and confidential communications with Cabinet, remained on these computers. Fortunately, in this case the charity recognized the failure on the part of the government entity and took immediate steps to have the information properly wiped from the EDSCs.

During the course of its preliminary inquiries, the OCC also learned that several office machines that had been used by another government entity (one that also deals with highly sensitive information) had been discarded and found their way to the Cayman Islands Red Cross Thrift Shop, where they would have gone on sale to the public. The OCC retrieved documents from these machines, which confirmed the use by the government entity. The EDSCs for each of the machines had not been removed by the entity either prior to discarding them in a hallway or before a third party transported them to the Red Cross. One of the machines contained a 40-gigabyte ("GB") hard drive.

While these two incidents may have been isolated, and the information contained on the EDSCs may not have been capable of causing any harm if placed in the public domain, they could just as easily have contained information that had national security implications.

Evidence was also received about the growing practice of mining the George Town Landfill for used computer parts, primarily hard drives, and the sale of recovered computer parts. The government's Computer Service Department ("CSD") is one of a number of organisations that dispose of computer equipment at the landfill, and thus its disposal practices were reviewed as part of this investigation.

Failure to properly dispose of EDSCs could result in the unauthorized release of personal information gathered by government (including medical records and personal financial information), as well as sensitive information about the operation of government, to persons who could use this information for improper purposes.

As a result of this preliminary evidence, the Commissioner determined that it was in the public interest to launch an own motion investigation to determine

put in other computers within government. He testified that once a hard drive was no longer of use to government, the CSD would take it to the landfill and destroy it with a sledgehammer. He added that the CSD did not remove the platter from the casing but simply smashed up the whole case.

2.5 Key findings

1. None of the Portfolios and Ministries investigated had a policy for addressing the disposal of EDSCs. It was also determined that none of the Ministries and Portfolios had sufficient procedures to demonstrate that they were properly managing and disposing of EDSCs.

2. With the exception of the Department of Tourism under the Ministry of Tourism and the Department of Education under the Ministry of Education, which had their own internal IT support functions for limited areas, all the Ministries and Portfolios claimed that they and their respective departments relied on the CSD to provide for the disposal of IT equipment including Blackberries when and if the need arose.

3. There was an overall lack of adequate documentation of EDSC disposal throughout the Ministries and Portfolios as well as at the CSD.

4. There was a general lack of awareness on the part of COs as to what should be done with EDSCs, as well as what was ultimately being done with EDSCs. Most of them were aware of their procedure for removing the actual asset from their asset registry, but once that process was completed there was no corporate memory and no further paper trail that could sufficiently verify what had happened to the EDSCs.

5. Until the launch of this investigation, the CSD would provide disposal services to any government department that requested this service. Once the computer had been properly removed from an entity's asset registry, the CSD would assess whether any parts could be salvaged for spare parts. This process included saving the hard drives if they could be used in other machines. These hard drives, if kept, were re-imaged. They would only be wiped if that process had been specifically requested by the entity. Once the computer had been stripped of any useful parts, the CSD would then take the remaining equipment to the landfill. While the CSD indicated that these machines were crushed, there was no way to verify if in fact that was being done. In the past, the CSD would only use a sledgehammer to smash hard drives deemed to be of no useful purpose.

6. It was apparent that communication between departments and CSD was not precise and that terminology was not used consistently. This may have resulted in a particular department seeking a higher level of service than was actually provided by the CSD.

7. This investigation revealed that COs were failing to take responsibility for adequately documenting and tracking the secure disposal of EDSCs. It appeared that the COs only ensured that assets were removed from the asset registries.

8. Data classification should be done, and be part of recycling and destruction process.

9. COs had not properly addressed the issue of the removal of government data once placed on civil servants' private computers.

2.6 Analysis

The lack of adequate documentation of EDSC disposal made it impossible to verify what equipment and how much equipment had been destroyed, as opposed to having been placed in a department storage container, given to a charity, sold to a member of staff, or thrown away in a dumpster.

The statement by CO Mr. Donovan Ebanks that a number of computers from his Portfolio had at one time been donated to the prison's educational program (and could not be verified as having been wiped), as well as the case of a private local charity that received computers from another government entity that still contained government files, led to the conclusion that some EDSCs had been released from the possession of the government and that all of them were not disposed of in a manner that ensured that the data was rendered inaccessible. The evidence of a lack of policy and procedure also led to the conclusion that, were it not for this investigation bringing the matter to the attention of COs, many other EDSCs would have been disposed of without ensuring that the data on them was rendered inaccessible.

It was clear that none of the Portfolios and Ministries were maintaining records of the use and ultimate disposal of EDSCs. The only records produced at the Portfolio/Ministry level related to the general disposal of the traditional physical assets. Ultimate responsibility for the tracking of the actual disposal of the EDSC was passed on to the CSD. While the CSD was able to provide some information regarding the assets that it had collected from the various departments, it did not have any record of what then happened to the EDSCs. Evidence from the CSD staff members exposed confusion and a lack of consensus on appropriate standards and procedures.

While the CSD potentially had the expertise to advise government on the recommended procedures for disposing of EDSCs, and in many instances may be the body requested to provide the service of disposal, the responsibility to ensure that EDSCs were adequately tracked through to final disposal rested with the COs.

The creation and implementation of a data classification system remains a project that should be completed. The failure to classify data and the resulting inability to know the level of care to be taken in decommissioning an EDSC impairs the design of an efficient and cost effective recycling and disposal process.

The use of personal computers and their retention of government information was an issue that was beyond the technical expertise of many of the COs interviewed. It is appropriate, then, to emphasize the need for this issue to be addressed while policy is developed. While it is true that the data transferred to a personal computer is still owned by government, and covered by confidentiality undertakings provided by government employees, arrangements must still be made for its proper disposal.

2.7 Conclusion

This own motion investigation by the OCC found that COs were not adequately tracking the use and disposal of EDSCs within their respective Ministries/Portfolios. Until the launch of this investigation by the OCC, very little attention had been given to the issue of secure disposal of EDSCs. It was clear that COs were unaware of what was being done with the EDSCs being disposed of from their Ministries/Portfolios and the departments under them.

While it has also become clear that not all EDSCs pose significant risk to the security of sensitive information, there is no way of clearly identifying which ones could pose a serious risk as information has not been classified. Regardless of what EDSCs are being considered, and regardless of what information is being stored on these containers, the process of tracking and monitoring the disposal of these containers has been insufficient to ensure that EDSCs are being disposed of properly.

As the COs have the responsibility of overseeing the assets of their Portfolio/Ministry as well as ensuring that records are being securely maintained, each Portfolio/Ministry must have a policy that provides for the secure maintenance and disposal of all EDSCs. However, the policy required for such a process need not be specifically designed to be unique to each Portfolio/Ministry and it is likely best that there be one policy developed for all of the public sector. The expertise required for the development of the policy potentially could come from the CSD, CINA and existing published works from abroad. It would be appropriate for the Chief Secretary to take oversight of this project. However, no objection would be raised if the issues were addressed as part of the current process to amend the Financial Regulations under the direction of the Financial Secretary.

What is a proper policy for the disposal of EDSCs? The new policy and procedures must protect private and sensitive information to a degree that is

commensurate with the risk of, and the damage caused by, unauthorized publication. It must include appropriate documentation that provides an auditable record trail from the introduction of the EDSCs into the government through to their final disposal, including appropriate evidence of what happens to the EDSC as it leaves government whether by donation to outside agencies, sale to individuals, or destruction. Responsibility for maintaining this paper trail falls to the COs. There are many well thought out policies available that could be referenced in the development of a policy for the Cayman Islands Government.

With the introduction of this enhanced practice of monitoring and secure disposal of EDSCs, there will be a need for all civil servants to be made aware of the importance of properly securing, maintaining, and disposing of all EDSCs.

2.8 Recommendations

It is recommended that:

1. Each Portfolio/Ministry have a policy on the use and proper disposal of EDSCs.
2. The policy for the use and proper disposal of EDSCs should be drafted in consultation with the CSD and CINA.
3. If a government entity does not use the CSD as its IT service provider, it must take steps to ensure that its service provider follows the new policy.

3. Introduction

Technological advances mean that information can be stored electronically by an ever growing number of devices. Often these devices are used in the course of everyday business and public sector activities. Sometimes, little thought is given to the type of information being collected, while it is often the case that few users have an understanding as to what information remains on the device when it has reached its functional life limit and is set out for disposal.

This report focuses on the disposal of electronic data storage containers ("EDSCs"). This class of device includes computer hard drives and memory chips in photocopiers, scanners, cameras, fax machines, cell phones and personal digital assistants (PDAs) including Blackberries. EDSCs also include floppy disks, diskettes, CDs, DVDs, USB thumb drives/jump drives, audio and video tapes and smart cards.

The Office of the Complaints Commissioner ("OCC") conducted some preliminary inquiries, which led to the conclusion that there was cause for concern about how EDSCs were being handled and ultimately disposed of by government.

The practices of many government entities regarding the secure disposal of EDSCs appeared not to be in accordance with reasonable disposal practices. For example, the OCC received testimony from a local charity that had been donated several used computers by a government entity that deals with highly sensitive information. As a matter of routine, the charity checked the computers to ensure they were in good order prior to putting them into service. During this check, the charity discovered that the government entity had not removed all government information from the computers. While the charity administrator did not open individual files, its testimony leads to the conclusion that many files, including some which may have contained very sensitive personal information, and confidential communications with Cabinet, remained on these computers. Fortunately, in this case the charity recognized the failure on the part of the government entity and took immediate steps to have the information properly wiped from the EDSCs.

During the course of its preliminary inquiries, the OCC also learned that several office machines that had been used by another government entity (one that also deals with highly sensitive information) had been discarded and found their way to the Cayman Islands Red Cross Thrift Shop, where they would have gone on sale to the public. The OCC retrieved documents from these machines, which confirmed the use by the government entity. The EDSCs for each of the machines had not been removed by the entity either prior to discarding them in a hallway or before a third party transported them to the Red Cross. One of the machines contained a 40-gigabyte ("GB") hard drive.

While these two incidents may have been isolated, and the information contained on the EDSCs may not have been capable of causing any harm if placed in the public domain, they could just as easily have contained information that had national security implications.

Evidence was also received about the growing practice of mining the George Town Landfill for used computer parts, primarily hard drives, and the sale of recovered computer parts. The government's Computer Service Department ("CSD") is one of a number of organisations that dispose of computer equipment at the landfill, and thus its disposal practices were reviewed as part of this investigation.

Failure to properly dispose of EDSCs could result in the unauthorized release of personal information gathered by government (including medical records and personal financial information), as well as sensitive information about the operation of government, to persons who could use this information for improper purposes.

As a result of this preliminary evidence, the Commissioner determined that it was in the public interest to launch an own motion investigation to determine

whether government was properly disposing of EDSCs when they were no longer of use to government.

The Commissioner decided that this investigation should be directed towards the Chief Officers ("COs") of the following entities: Cabinet Office; Portfolio of the Civil Service; Portfolio of Internal and External Affairs; Portfolio of Finance and Economics; Ministry of Education, Training, Employment, Youth, Sports and Culture; Ministry of Tourism, Environment, Investment and Commerce; Ministry of District Administration, Planning, Agriculture and Housing; Ministry of Communications, Works and Infrastructure; and the Ministry of Health and Human Services. This decision was taken because, under the Public Management and Finance Law (2005), it is the responsibility of COs to dispose of government assets in a proper manner. Also, each CO needs to implement an appropriate system of internal controls in accordance with the Financial Regulations (2008 Revision) PART VII Section 29:

"A chief officer of a prescribed entity shall ensure that an appropriate system of internal controls operates within the entity and that the system is adequate to safeguard the entity or executive resources for which the prescribed entity is responsible"

Assets are publicly owned and must be accounted for during their use or disposal (Financial Regulations 2008 Third Schedule, part 8 page 108). Data that is stored in the asset must be protected and contracts of use of software must be honoured. (Public Management Law 2007 section 5 and the Freedom of Information Law section 23.)

For the purpose of this investigation, the offices of the Auditor General and Attorney General were excluded as their offices do not fall under the OCC's jurisdiction. However, while these offices were excluded, the OCC encourages the COs of both to carefully consider their practices regarding the proper disposal of EDSCs in the light of the findings of this investigation.

The questions of value for money and the recycling of computer equipment, and the environmental impact of the disposal of computer equipment, were not addressed by this investigation. For a useful discussion of some of these topics, see the report published by the National Audit Office (UK) titled: "Improving disposal of public sector information, communication and technology equipment" (31 July 2007, www.noa.org.uk/publications/0607) and the book by Ruediger Kuehr & Eric Williams (editors): Computers and the Environment: Understanding and Managing Their Impacts (Kluwer Academic Publishers, 2003, ISBN 1-4020-1680-8.).

4. Background

Electronic equipment that in the past may not have stored information now has that capacity. Early in this investigation, this Office retrieved a 40GB hard drive from a photocopier that was on offer for sale at the Red Cross

Thrift Shop. That copier was thus capable of storing a significant amount of government information.

The amount and types of information stored on these items varies greatly, but the information stored on any of these EDSCs needs to be carefully considered both during their use as well as during their disposal.

In some cases, the owner of the EDSC may believe that the information contained on the item is not of any significant value if it falls into the hands of other persons. They may therefore choose to simply discard the item without ensuring the device is destroyed or that all possible information has been removed prior to passing the EDSC to another user. In other cases, information on these items could cause the owner or subject of the data considerable hardship, embarrassment or legal ramifications if it is left for others to retrieve.

Computer hard drives are capable of storing vast amounts of information. Even when the user is accessing information over the internet, with a Citrix token (a security device that allows secure access to the government network), or using a thumb drive, an image of the file that they are working on is transferred to their computer, or whatever computer they are working on at that moment. While these images are not easily accessible using standard methods of file retrieval once the token or thumb drive is removed or the internet connection is broken, the information is still on the computer; if a person that wishes to retrieve that information was able to gain access to the hard drive they could, with relatively inexpensive software (in some cases freely available over the internet), access those documents.

One of the most popular pieces of electronic equipment for many civil servants today is the Blackberry, which is used to access documents and emails, make calls, send text messages and even edit documents. A great deal of information is stored on these devices, and while considerable effort has been taken by their manufacturer, Research In Motion, to safeguard the privacy of the user, it is not clear how much information remains on the EDSC even after it has been cleared using the "wipe" feature on the phone.

USB memory sticks, also known as 'thumb drives' or 'jump drives', are also becoming popular with civil servants. They allow a person to carry with them hundreds of files. For less than $50, a person can buy an 8GB jump drive, which is more than enough memory to save all of the word-processing files typically handled by a civil servant in a year. Yet it is not uncommon for these jump drives to go missing. They are small and often treated with no greater concern than a pen or pencil carried away from the office. The OCC has witnessed jump drives tossed into vehicles, purses, and gym bags.

In order to ensure that information contained on EDSCs is protected against unauthorized access, the devices must be adequately tracked and secured. Once the devices have reached the end of their usefulness, carefully considered steps must be taken to remove information prior to disposal. In some cases, the devices must be destroyed in order to adequately protect the information that may remain on them.

Governments in other parts of the world have realized just how much information is being saved on EDSCs and have put in place procedures to better monitor their secure processing from beginning of their lifetime to the end. For example, the United States Defense Security Service, an agency of the Department of Defense, published the National Industrial Security Program Operating Manual (2006 – updated regularly over the past decade; www.dss.mil/GW/ShowBinary/DSS/isp/fac_clear/download_nispom.html). Also, the Department of Commerce (USA), National Institute of Standards and Technology published a "Guideline for Media Sanitization: Computer Security" (NIST Special Publication 800-88, http://csrc.nist.gov/publications/PubsSPs.html). It contains, at page 17, a useful media sanitization decision matrix chart. The Communications and Electronics Security Group of the UK's GCHQ also has established data removal standards, although they are not mandatory (www.cesg.gov.uk/policy_technologies/policy/policy.shtml; available only by direct request). A number of provincial government offices in Canada also have addressed the issue. The simple yet clear "Electronic Media Disposal Standards and Procedures" for the Province of Manitoba Government was of interest as it addressed the pertinent issues in less technical language (not on their website). While the OCC is not endorsing a particular procedure we recognize the need to establish written guidelines. The Cayman Islands Government must determine the level of and procedure for the secure wiping or disposal of EDSCs.

Locally, at least one public entity, the Cayman Islands National Archive ("CINA"), has begun to consider the issue. The National Archive and Public Management Law 2007 is in effect a stop order against the disposal of records in any format. The law provides that records can only be disposed of after approval of the Advisory Board. The Board will also have the role of approving schedules of guidance on the destruction of records, which currently are being finished. (The schedule will then go to the Chief Secretary for approval and then to Cabinet for approval.) The schedule of guidance on disposal in relation to information technology and management (including maintaining and disposing of software or hardware, and creating, storing and disposing of information resources) is due to be written and approved by October 2009.

There are several terms used throughout this report that warrant clarification:

1. 'Wipe' is a term commonly used to mean the removal of information from EDSCs. For the purposes of this investigation, 'wipe' refers to the EDSC being essentially cleaned of all stored information. It has been recognized that even with wiping to mid-level standards (see below) it is possible that in a laboratory setting some trace elements of information could still be recovered.

2. 'Re-Imaging' is a term used when the computer operating system and applications are reinstalled on a computer. While this action removes the links to the data files that are on the hard drive, it does not actually remove the old files.

3. 'Ghosting' is a term used when the entire content of an existing hard drive is copied and transferred to another media such as another hard drive.

4. 'Degaussing' is the process of decreasing or eliminating an unwanted magnetic field, which effectively eliminates ("purges") all data from EDSCs.

There are various wiping schemes ("algorithms") including:

- British HMG IS5 (Baseline) (1 pass): Data is overwritten with zeroes with verification

- Russian GOST P50739-95 (2 passes): This shredding algorithm calls for a single pass of zeroes followed by a single pass of random bytes.

- British HMG IS5 (Enhanced): A three pass overwriting algorithm – first pass with zeroes, second pass with ones and the last pass with random bytes (last pass is verified).

- US Army AR380-19: This is a data-shredding algorithm specified and published by the U.S. Army. It is a three pass overwriting algorithm – first pass with random bytes, second and third passes with certain bytes and with its compliment (with last pass verification).

- US Department of Defense DoD 5220.22-M: This is a three pass overwriting algorithm – first pass with zeroes, second pass with ones and the last pass with random bytes. With all passes, verification. (Note: the current edition no longer prescribes wiping methods, but leaves the decision to the "Cognizant" Security Authority.)

- US Department of Defense DoD 5220.22-M (E): This is a three pass overwriting algorithm – first pass with certain bytes, second pass with its complement, and the last pass with random bytes (see note above).

- US Department of Defense DoD 5220.22-M(ECE): This is a seven pass overwriting algorithm – first and second passes with certain bytes and with its compliment, then two passes with random character, then two passes with character and its complement and the last pass with random characters (see note above).

- Canadian RCMP TSSIT OPS-II: This is a seven pass overwriting algorithm with three alternating patterns of zeroes and ones and the last pass with random characters (with last pass verification).

- German VSITR: This seven pass algorithm calls for each sector to be overwritten with three alternating patterns of zeroes and ones and in the last pass with character.

(source: www.fileshredderpro.com/shredding-algorithms.html)

5. Purpose of Investigation

The purpose of this investigation was to determine whether the Portfolios and Ministries investigated had a policy for addressing the disposal of EDSCs; whether that policy, if it existed, was being followed; if there was no policy, what actions were being taken by the various Portfolios/Ministries; and to consider whether the process being followed was adequate for the proper disposal of EDSCs.

Ensuring that all government Portfolios and Ministries have a proper disposal policy, and that they are adequately administering that policy, provides greater protection of information and accountability of government for how it is handling that information.

While the primary purpose was achieved through this investigation, we also found that this investigation served to provide considerable opportunity for raising the awareness of the relevant issues among COs and CSD management, as well as the various other government officials interviewed in relation to this matter.

As this Office anticipated that most, if not all, COs would have service level agreements ("SLAs") with the CSD, this investigation paid particular attention to the procedures followed by CSD for the disposal of EDSCs.

The investigation also brought to the forefront an issue that had once been championed by CSD but had not been progressed: the issue of the classification of information held by government (i.e., privacy or security classifications such as restricted, confidential, secret, top secret) and the methods by which each classification of information is safeguarded, including the piece of paper or EDSC that once was the primary holder of that

information. In brief, confidential information, while requiring protection, need not be secured in the same fashion as information that would jeopardize national security, while an EDSC that held no private information, such as a device that stored only weather reports, could be given away as is.

6. Method

On 23 January 2009, the COs for the Cabinet Office; Portfolio of the Civil Service; Portfolio of Internal and External Affairs; Portfolio of Finance and Economics; Ministry of Education, Training, Employment, Youth, Sports and Culture; Ministry of Tourism, Environment, Investment and Commerce; Ministry of District Administration, Planning, Agriculture and Housing; Ministry of Communications, Works and Infrastructure; and the Ministry of Health and Human Services were notified in writing of this own motion investigation. At that time, they were all requested to provide to the OCC a formal written response, which was to include:

1. The policy of their Portfolio/Ministry as a whole for the disposal of EDSCs. This was to include each department's policy if they had been delegated that responsibility and proof of that delegation.
2. If their policy was to turn over EDSCs to the CSD for disposal, they were to provide a copy of their SLA.
3. If they had no policy, they were requested to provide information on what was done with EDSCs that were no longer in use.

A subsequent letter was sent to the COs on 30 January 2009 requesting that they also provide this Office with the following information:

1. A list of all EDSCs that their Portfolio/Ministry had disposed of and the corresponding records of disposal. This was to include the disposal records for all entities under their Portfolio/Ministry.
2. How did their Portfolio/Ministry's policy/practices address the voluntary use of staff members' privately owned EDSCs, e.g., home PC, personal PDAs or other personal EDSCs that they may have used for government business?
3. To provide the names and contact information of all the companies/service providers, if any, that had provided IT services to their Portfolio/Ministry when disposal or replacement of EDSCs had been required.
4. Where did they store their retired IT equipment before it was disposed of permanently?
5. Where they disposed of their retired IT equipment.
6. If they did not use CSD for the disposal of EDSCs, what software was used by their service provider to conduct the wiping/cleaning of the EDSCs?

All of the information requested through the letters of 23 January 2009 and 30 January 2009 was to have been provided to the OCC no later than 9 February 2009.

Documentation from COs, as well as other pertinent information, was reviewed prior to conducting face-to-face interviews with the COs and/or their delegates.

Upon completing the majority of interviews with the COs, interviews with various CSD officers were conducted. These interviews included observation of procedures for wiping and disposing of EDSCs.

In the course of this investigation, a few EDSCs were seized and reviewed by our expert retained from Deloitte.

7. Findings

7.1. Cabinet Office

The Cabinet Office does not have a policy for the disposal of EDSCs.

Cabinet Office CO Orrett Connor confirmed this during his interview with this Office on 18 February 2009. He stated that the Cabinet Office relied on the CSD to provide disposal of all computer equipment. CO Connor also stated that the Cabinet Office did not have any procedures regarding the disposal of other EDSCs, such as DVDs, jump drives and smart cards.

CO Connor stated that the CSD addressed all of the computer and Blackberry related service issues for the Cabinet Office. He was not aware of what was done with any of these items once CSD took charge of them. He confirmed that while he was responsible for signing off on the disposed assets for the various departments under and within the Cabinet Office, responsibility for them passed to the CSD once they were removed from the fixed asset registry.

CO Connor stated that he was not aware of what the departments under the Cabinet Office did with their EDSCs but committed to getting this information and passing it on to the OCC. Subsequent information provided by the Cabinet Office confirmed that adequate tracking records were not being maintained for the disposal of EDSCs.

CO Connor admitted that most record keeping on transactions for the disposal of EDSCs once disposed from the asset registry of the Cabinet Office had been left up to the CSD to generate.

The Cabinet Office has not addressed the use of personal computers for government work carried out at home. But it recognized the potential for

government information being saved on personal computers if officers were doing work at home, and the safe disposal concerns this might raise.

He concluded by stating: "I recognize that there are areas for improvement and we will continue to work with Computer Services to introduce and implement a comprehensive set of policies and procedures for the handling and disposal of EDSCs."

7.2. Portfolio of Internal and External Affairs

The Portfolio of Internal and External Affairs does not have a policy for the disposal of EDSCs.

The Portfolio's CO, Mr. Donovan Ebanks, confirmed during his interview with this Office on 3 March 2009 that while he had not gathered the information requested by the OCC regarding the practices of the various departments under the Portfolio on disposal of EDSCs and subsequent records, he felt certain that any records that might have been made would be limited to computers. He admitted that very little tracking of EDSCs had been conducted up to this point in time.

CO Ebanks stated that very little consideration had been given to the EDSCs contained in Blackberries. He commented that there had not been, in his opinion, a consciousness regarding the amount of information stored on these devices, although he had not seen this as a major security concern.

He stated that the issues raised by this Office regarding the secure disposal of EDSCs had focused due attention on the issue. He admitted that there was a need to revisit the Portfolio's practices, including a review of the SLAs with the CSD for the coming financial year. He felt that the proper disposal of EDSCs needed to be specifically addressed within the SLAs. He also noted that the Portfolio may need to look to the CSD to provide additional oversight with regard to other types of machines that had EDSCs that may not be serviced by the CSD but required CSD expertise to ensure that stored information was adequately removed prior to disposal.

He stated that the Portfolio had not made any of its computers available to the public for purchase or as donations. He did recall an occasion when a number of computers were donated to the prison's educational program, but admitted that he was not aware of what they were being used for at the prison nor was he aware of what was done with them prior to sending them out to he prison. When asked if there were any records of this transaction, he stated that there was unlikely to be any documentation.

While he admitted that records on the disposal of EDSCs was likely to be minimal, he endeavoured to gather what information he could from each of the departments under his Portfolio, in addition to the other information

requested by the OCC by 6 March 2009. To date, this information has not been provided. As a result, the OCC has surmised that no records had been created which adequately tracked the disposal of EDSCs.

CO Ebanks stated that the Portfolio relies on the CSD to address all of its computer issues and if a machine could not be fixed, then arrangements were made through the CSD to replace that machine and dispose of the old one. He noted that any documentation regarding this disposal would be kept by the CSD.

He noted that while this was still an important issue, the fact that the Freedom of Information Law has been implemented has created a situation where more information than ever before is open to the public. Regardless, he agreed that the government did not want to be providing information through improper EDSC disposal practices.

CO Ebanks understood the concerns associated with the improper disposal of EDSCs, as well as the risk of information left on civil servants' computers at home not being properly disposed of, and said he believed that the government had reached a point where it must look closer at its practices to ensure that these items were being tracked and disposed of properly.

7.3. Portfolio of Finance and Economics

The Portfolio of Finance and Economics does not have a policy that adequately addresses the proper disposal of EDSCs.

The Portfolio's CO, Mrs. Sonia McLaughlin, provided its Asset Disposal Policy on 12 February 2009 when meeting with the OCC. She presented it as the policy that the Portfolio used to dispose of assets. In reviewing with CO McLaughlin and her Senior Assistant Financial Secretary, Ms. Anne Owens, it became apparent that this policy did not specifically address the disposal of the EDSCs.

The Portfolio recognized that it needed to take steps to ensure that its procedures regarding the proper disposal of EDSCs were improved. CO McLaughlin stated that the Portfolio relied on the professional expertise of the CSD to provide for the proper disposal of its computer equipment. While the Portfolio's SLA with the CSD did not provide specific reference to the disposal of EDSCs, CO McLaughlin stated that the CSD had in the past disposed of computers for the Portfolio. To her knowledge, there had not been any additional fee for that service.

The evidence provided by this Portfolio demonstrated that it had used initiative to properly document the disposal of computer assets, but also demonstrated that the current process does not allow for the disposal of EDSCs.

CO McLaughlin stated that her Portfolio would be looking closely at its procedures as they related to EDSCs to ensure that they were being tracked and disposed of properly. She said she saw the wisdom in, and indeed proposed, the development of a central policy for all of government. She noted that the Financial Regulations were being reviewed and suggested that it may be timely to look at changes that would include specific practices involving the proper disposal of EDSCs.

While the Portfolio felt certain its various departments were properly storing EDSCs, it could not state definitively where each department stored these items.

The Portfolio provided a list of 24 electronic items that had been disposed of by its departments since 1 January 2007. It stated that it had at times sold computers to persons working within the Portfolio and had donated computers to one of the schools. However, SAFS Owens admitted that while the practice was to have these machines wiped first by the CSD, there was no record of this having been done.

CO McLaughlin stated that the Portfolio had the kind of relationship with the CSD that meant it did not consider it necessary to do much more than request that CSD officers came and took care of its computer issues. It never considered that it should be more formally documenting those transactions. CO McLaughlin suggested that the CSD could provide a specific report, which could be attached to the disposal record outlining what exactly, was done with each EDSC and related computer equipment.

The Portfolio stated that it had not disposed of any cell phones. It noted that, typically, cell phones which were no longer in use by the Portfolio were secured within the Portfolio offices. It provided the OCC with a Blackberry for testing that had been "wiped" in order to determine whether the wiping feature on the Blackberry did indeed clear the information on the phone (see below).

The Portfolio had not addressed the use of personal computers for government work done at home but recognized the potential for government information being saved on personal computers if officers were doing work at home.

SAFS Owens stated that the Portfolio had disposed of a photocopier that was no longer of any use. It was then taken by Public Works to be disposed of, presumably at the landfill. However, she admitted that there was no record confirming that the machine was actually disposed of there and no steps had been taken to check that information that may have been stored on the machine had been wiped.

SAFS Owens also noted that only the Portfolio's computers and cell phones were serviced through the CSD.

7.4. Portfolio of Civil Service

The Portfolio of the Civil Service does not have a written policy relating directly to the disposal of EDSCs. This was confirmed to the OCC at a meeting with the Portfolio's CO, Mrs. Mary Rodrigues, and the Portfolio's chief financial officer (CFO), Mr. Matthew Tibbetts, on 6 February 2009.

CFO Tibbetts noted that the Portfolio was relatively young, having been established only in November 2004, and as a result the majority of its equipment was relatively new. Only one computer had been disposed of to date. The documentation on that disposal, which happened in 2005, was provided to this Office, but while the documentation provided evidence that the computer had been removed from the Portfolio's Asset Registry and given to CSD for disposal, the documentation did not provide any information as to what CSD did with the computer or the EDSC. CFO Tibbetts stated that the CSD informed him that if a hard drive were in working order, the CSD would wipe the hard drive; however, if the hard drive were not functioning or no longer of use it would use a sledgehammer to destroy it. However, neither CO Rodrigues nor CFO Tibbetts knew what the CSD had done with the computer. CO Rodrigues noted that the disposal of that asset occurred prior to her and the CFO joining the Portfolio. CFO Tibbetts stated that it was the Portfolio's expectation that CSD, as a central provider of disposal services for IT equipment, would provide a good quality service.

As a result of this investigation, CO Rodrigues recognized the need to properly track and document the actions taken in disposing of EDSCs from the Portfolio. CFO Tibbetts confirmed that all EDSCs would continue to be referred for destruction, when that time came, through the CSD.

CO Rodrigues committed to working with any recommendations made by the OCC to ensure that the Portfolio's policies were in keeping with best practice for the disposal of EDSCs.

CFO Tibbetts noted that the Portfolio had an old fax machine that was no longer in use but was secured within the office. In light of this investigation, he said that the Portfolio would ensure that it consulted with the CSD to ensure that any EDSC that may be in the machine had been wiped or destroyed prior to final disposal.

CO Rodrigues stated that all cell phones for the Portfolio that were no longer in use had been retained and secured within the Portfolio office.

CO Rodrigues and CFO Tibbetts stated that in future, they would continue to consult with CSD on EDSC disposals and would ensure that they send all equipment containing EDSCs to the CSD for disposal once they had become either dysfunctional or for some other reason no longer of use to the Portfolio. The Portfolio would also consider the issue of government information being stored on employees' home computers and the issue of the proper disposal of those EDSCs.

It was acknowledged by the CO and CFO that although information on assets that had been disposed of were maintained in the asset registry, their record keeping procedures regarding actions taken in the physical disposal of EDSCs required attention to ensure that better tracking could be achieved.

7.5. Ministry of Health and Human Services

The Ministry of Health and Human Services does not have a policy that adequately addresses the proper disposal of EDSCs.

During an interview with the OCC on 11 February 2009, CO Mrs. Diane Montoya stated that the Ministry did not have a written policy but that it did have a procedure. However, a review of information subsequently provided revealed that the procedure encompassed only the disposal of assets and did not include specifics regarding the final physical disposal of EDSCs.

CO Montoya stated that the Ministry did not have many of the items listed as EDSCs and therefore had not considered the need to track those items. CO Montoya stated that the Ministry used jump drives only in the case that there was a storm threat to secure important documents that would be needed to quickly be able to progress work after the storm.

She confirmed that the Ministry relied on the CSD to dispose of EDSCs. However, she stated that most of the Ministry's equipment had not been disposed of, since the machines were usually passed around until they were no longer of any use, thereby extending the period of use.

She stated that the Ministry had only ever disposed of one cell phone, which was done through the CSD. She was unable to confirm what happened to the cell phone once it returned to the CSD.

The Compliance Manager for the Ministry, Mr. Daniell Rattan, provided documentation subsequent to the interview with the CO which provided more information regarding the items disposed of through the Ministry. While the documentation provided information about several items that had been disposed of, several of the departments under this Ministry responded indicating that they had not disposed of any EDSCs. The departments that did provide evidence of items having been disposed lacked sufficient detail as to what was actually done with the EDSCs.

CO Montoya stated that this investigation had been helpful to her Ministry, as it had highlighted many of the issues that it needed to consider regarding the secure use and disposal of EDSCs. She commented that she had never even considered the disposal practices for many of the EDSCs that were listed in the OCC's opening letters to the COs. She also confirmed that she did not know what happened to the equipment once it was entrusted to the CSD for disposal.

7.6. Ministry of Education

The Ministry of Education, Training, Employment, Youth, Sports and Culture did not have a policy for the disposal of EDSCs in January 2009, but it immediately upgraded an existing policy in an attempt to address the issue. While this investigation revealed that additional work was needed to more effectively address the disposal of EDSCs within this Ministry, the OCC recognized the deliberate efforts of the Ministry to address the problem.

The information technology for government schools was managed separately, and that unit had a policy, which, with some modification, was satisfactory. (An expert retained by the OCC confirmed that the computer had been wiped successfully and that the way it had been disposed of by one of the schools complied with the policy.)

Acting CO Mr. Stran Bodden stated during the OCC's interview with the Ministry on 12 February 2009 that he was not aware if the Ministry did have records of what the CSD had done with the Ministry's computers once they had been identified for disposal. He noted that the Ministry relied on the expertise of the CSD to properly dispose of EDSCs.

While some of the documents provided by the Ministry identified in part what had been done with the EDSCs of the computers that had been discarded, the documentation failed to cover the process through to the final disposal and was not consistently documented for each disposal form. The records provided information on assets that had been removed from the asset register, but the Ministry was unable to confirm where those items ended up for final disposal.

The Ministry has not addressed the use of personal computers for government work done at home. But the Ministry recognized the potential for government information being saved on personal computers if officers were doing work at home, and the need to have a policy for disposal of that information.

7.7. Ministry of District Administration, Planning, Agriculture and Housing

The Ministry of District Administration, Planning, Agriculture and Housing does not have a policy that addresses the disposal of EDSCs. However, the Ministry stated that it did have an SLA with the CSD to provide support for its Blackberries and computers.

The Acting CO for the Ministry, Ms. Jennifer Ahearn, stated in an interview with the OCC that the Ministry relied on the expertise of the CSD to take appropriate actions in the disposal of the EDSCs. She stated that she did not know what happened to EDSCs once they were removed from the asset registry and turned over to the CSD. However, she stated that most of the EDSCs had been retained within the various departments under the Ministry and had been appropriately secured within locked offices.

The Ministry provided information on the various departments' practices and EDSCs that had been disposed of. While, in most cases, the Ministry was able to identify the equipment that had been disposed of, it was not able to provide specific information detailing whether the EDSCs had been placed in storage or had been destroyed. The storage of government information on home computers and properly disposing of those EDSCs remained an open question.

Acting CO Ahearn acknowledged that EDSCs needed to be better tracked to ensure that they were properly secured during use as well as properly disposed of. She noted in her response to the OCC on 9 February 2009 that perhaps the government should develop a "centralized, uniform, prescriptive policy specific to the disposal of EDSCs".

7.8. Ministry of Communications, Works and Infrastructure

The Ministry of Communications, Works and Infrastructure does not have a policy that addresses the disposal of EDSCs. The CO, Mr. Carson Ebanks, confirmed this in his letter to the OCC dated 28 January 2009.

He noted that the practice within the Ministry had been to request EDSC disposal services from the CSD when needed. In his letter to the OCC dated 18 February 2009, he noted that before any computers left the Ministry, the CSD was asked to "erase/clean the hard-drive". He noted that, with the exception of a few pieces of IT equipment noted in the response, the Ministry had kept its retired IT equipment. He noted that retained equipment had been secured in the offices of the Ministry and its departments.

The Ministry seemed to be aware of the IT equipment that it had, and those items that it had disposed of. However, the records provided did not give

clear information as to what was ultimately done with the EDSCs that were disposed of. CO Ebanks was not able to provide information about what was done with EDSCs once they had been turned over to the CSD.

While the review of the information provided by the various departments under this Ministry revealed that there were very few records of having been disposed of, it was also evident that adequate records of EDSCs were not being maintained. The CO wrote that the Ministry would have a physical inventory of fixed assets, which will include some of the EDSC assets, once it can be uploaded in the IRIS System.

7.9. Ministry of Tourism, Environment, Investment and Commerce

The Ministry of Tourism, Environment, Investment and Commerce does not have a policy that addresses the disposal of EDSCs.

The CO for the Ministry, Ms. Gloria McField-Nixon, stated during her interview with the OCC on 19 February 2009 that the Ministry relied on the technical expertise of the CSD to ensure that its computers and Blackberries were wiped clean before being discarding. She went on to state that the Ministry did not have a separate policy addressing the use and disposal of EDSCs. It was her belief that these policies came under a central policy put into practice by the CSD.

She stated that, with the exception of the Department of Tourism, which had its own IT support function, all other departments under this Ministry relied on the CSD for their IT support.

She stated that officers with Citrix tokens would occasionally use internet cafes and hotel business centres to access the Ministry's network while away from the Cayman Islands, although only if they were on personal leave and needed to respond to an urgent matter – otherwise, they would respond from their government-issued laptop computer. (She did acknowledge that a copy of a document downloaded to the remote computer remained on that computer, even if the link to it was deleted, although she said that she did not believe this amounted to a significant risk to confidentiality obligations.)

The Ministry relied on the CSD to provide disposal services when and if those services were required. If the EDSC were not being disposed of, it would be stored within the offices of the Ministry or the departments under the Ministry.

On the matter of Blackberries, CO McField-Nixon stated that her own device had the ability to edit documents and send them back to other users. As someone who travels regularly with her job, she noted that remote access had become a necessity. She recognized that this could create a situation where

strict control over document security could be compromised, but felt that in most cases the documents being processed remotely would not be sensitive.

She stated that her Ministry considered the CSD to be the government's chief advisor with regard to technology, and therefore would expect that the CSD would set the rules for all IT related issues including the disposal of EDSCs.

From this investigation, it was evident that adequate records were not being kept of the use and disposal of EDSCs within this Ministry. CO McField-Nixon stated that the only log kept regarding any EDSCs would be its Asset Disposal log. But this did not provide any specific information regarding the actual disposal of EDSCs. Her evidence was that the last disposal occurred in 2006 when the computers though out the office were replaced.

CO McField-Nixon reported that while all the departments under the Ministry were using the CSD for the cleaning of information from any EDSC earmarked for disposal, in practice the Ministry was keeping the equipment for a period of time before sending it to the landfill.

7.10. Summary of findings from Portfolios and Ministries

As a result of interviews with and written responses from these nine COs, we were able to confirm that none of them had a policy addressing the disposal of EDSCs. It was also evident that they were not adequately documenting the process of EDSC disposal.

With the exception of the Department of Education and the Department of Tourism, which both have internal IT functions, all of the Ministries and Portfolios investigated relied upon the CSD to provide IT services including the wiping of hard drives and the disposal of machines. Some COs also claimed to use the CSD for the wiping of their Blackberry devices once they were being replaced.

The Ministries and Portfolios claimed to rely on the CSD to appropriately dispose of any EDSCs given to them for disposal. Yet none of them was able to verify what was actually done with any of the EDSCs that were removed from their asset registries. The records indicated only that the items had been disposed of from the asset registry. No information existed verifying that the EDSC had been passed to another user, for instance, wiped and kept as a spare by the CSD, destroyed and disposed of at the landfill, or the subject of any other specific action.

While several of the COs were not aware of the section of their SLAs that covered the disposal of EDSCs, all claimed to have had those services provided, without additional charges by the CSD. On checking with the CSD, several of the COs were able to confirm that disposal of EDSCs was

covered under section CSD-0018-01 (PC Infrastructure Service and Technical Support).

All of the COs recognized the value in having an EDSC policy, and were receptive to ensuring that a properly established policy would be implemented within their respective Ministries and Portfolios.

None of the Ministries and Portfolios had implemented practices to adequately monitor the overall use and disposal of EDSCs in general. The only items that had been tracked, at least in part, were computers and Blackberries.

Many of the departments within government claimed to have not disposed of any EDSCs. Many of these items that were no longer in use were said to be stored within the various offices and rented storage units of the departments. However, this could not be verified, as there was a lack of sufficient documentation detailing the location of the items no longer in use. And at least one Ministry (Tourism) admitted to having sent computers to the landfill after the CSD had processed them.

The Ministries and Portfolios had also not dealt with the question of information transferred from work being left on civil servants' home computers.

7.11. Findings from the CSD

Ministries and Portfolios use the CSD for the servicing and support of their IT equipment, as well as network support for their Blackberry services. Early in this investigation, it became evident that Ministries and Portfolios also relied on the CSD to recycle and dispose of hard drives. They were notably reliant on the CSD's quality of service, and for the appropriate documentation of any of the services.

The COs and the CSD noted that the disposal and servicing of other EDSCs, such as jump drives, CDs, photocopiers, fax machines, etc., had not in the past been done through the CSD.

7.11.1 Records

This investigation has determined that the CSD has not been adequately documenting and tracking the storage and disposal of discarded computer equipment entrusted to it by the various departments of government. Interviews with various CSD officials resulted in a general consensus that the Department's procedures required improvement in order to better track and document the final disposal of any EDSCs entrusted to it.

The primary interview with the CSD was conducted on 19 February 2009 with the Deputy Director of the CSD responsible for cover operations and

networking, Mr. Wesley Howell, the Deputy Director responsible for technical support and help desk, Mr. Rex Whittaker, and the Security Analyst for operations including IT security, Mr. Brian Nimmo. (The Director of the CSD, Mr. Gilbert McLaughlin, confirmed in a telephone conversation with the OCC early on 19 February that he would be unable to attend the meeting but stated that the officers attending would represent the CSD and could speak for him.)

During this meeting, DD Whittaker admitted that the CSD had not been maintaining records to a standard that would allow for proper tracking of EDSCs through to final destruction. He noted that at the time of this interview, the CSD had begun to develop a more structured process of documenting and tracking the disposal process. He recognized that a more substantial audit trail needed to be developed in order to ensure that an accurate accounting could be provided for all EDSCs entrusted to the Department for wiping or disposal.

7.11.2 Quality of Service

DD Howell stated that CSD procedures for wiping computer hard drives was "loosely based on (US) Department of Defense (DOD) standards", and that wiping of hard drives was carried out using software called Darik's Boot and Nuke ("DBAN"), an 'open source' program. He pointed out that disk-wiping programs could only be used if the hard drive was still functioning.

Security Analyst Nimmo stated that DOD standards for wiping hard drives required seven or eight 'passes' with the wiping software – whereby the previous data is overwritten seven or eight times by random data. DD Howell stated that the CSD's standard was to do 10 passes with the wiping program.

DD Whittaker stated on 19 February 2009 that the CSD used DBAN for wiping hard drives. However, CSD technician Simon Gunn told the OCC on 5 March 2009 that the Department had acquired a new program called Kill Disk in the previous week. He stated that the change to the new software was due in part to the fact that it was a commercial program, and therefore product support could be more readily attained. He also stated that the new program was capable of performing the same 10 passes as DBAN but in far less time.

Mr. Gunn proceeded to demonstrate the new process that the CSD would be following for wiping a hard drive. It took a little over four hours to complete, and when the program was finished running, the program displayed a message confirming that 10 passes had been made and that the operation had been 100% successful. In order to independently verify this, the OCC took possession of the wiped hard drive and passed it to experts. Mr. Chris Rowland of Deloitte subsequently reported that the wiping process had indeed been a success and no useful data remained on the hard drive.

On 19 February 2009, DD Whittaker stated that if a hard drive could still be used, the CSD would "ghost" and "re-image" the hard drive. This process, according to DD Whittaker, simply erased the directory so that files could not be read from the computer. However, he acknowledged that when this process was carried out, all the files that were on the hard drive were still there until they would remain there until they were eventually written over by new files.

DD Whittaker stated that it had been the practice of the CSD that only hard drives that were still going to be used within government were re-imaged, and were often used for parts to be put in other computers within government. He also testified that once a hard drive was no longer of use to government, the CSD would take it to the landfill and destroy it with a sledgehammer. He also stated that the CSD did not remove the platter from the casing but simply smashed up the whole case.

On 5 March 2009, the OCC witnessed the whole process followed by the CSD for destroying a hard drive. While DD Whittaker stated that the past process of destroying a hard drive did not include wiping the data first, the new procedure demonstrated to the OCC did in fact include wiping the hard drive. After this, three half-inch holes were drilled through the hard drive box and platters inside the box, before the apparatus was finally shattered by a sledgehammer. The demonstrated procedure also included witnessed documentation of the entire process.

7.11.3 External control

While the CSD demonstrated its understanding and interest in changing its procedures to ensure more secure disposal of EDSCs, DD Howell noted that the Department could not mandate that all EDSCs be brought to them for disposal. He pointed out that EDSCs were the property of each Portfolio/Ministry.

In addition, DD Howell and DD Whittaker revealed that very few EDSCs had been provided to the CSD for disposal in the past. DD Howell pointed out that the CSD had received several enquiries from government entities about the Department providing this service since the OCC investigation began.

During a visit by the OCC to the CSD on 5 March 2009, the Support & Helpdesk Project Manager, Mr. Clemence Spence, stated that the CSD seldom actually received EDSCs back from the various departments once the Department had recommended that those items be condemned. He noted that once the CSD had recommended that the old machine be condemned, the departments still needed to complete a form indicating they wished for the CSD to collect the old machine for disposal. He stated that the computers

that were no longer in service were still the asset of the department and therefore could not be taken by the CSD without authorization.

7.11.4 Internal controls

While DD Whittaker claimed during the CSD interview with the OCC on 19 February 2009 that he had a list of all the EDSCs that the CSD had disposed of for all government entities, he later clarified that the list was actually individual memos from various departments requesting that the CSD remove old computers. He stated that while the memos contained specific information about the machines, such as serial numbers, the CSD did not maintain any records of what happened to the machines once they had been collected.

DD Howell confirmed that the CSD had now started drafting a chain of custody of evidence document into the Department's more formal procedures.

The CSD is now proposing that, in light of the fact that information is not currently classified; all drives once condemned should be degaussed and physically destroyed. However, DD Howell highlighted the fact that the CSD could only ensure that proper disposal occurred if the machines were given to them for destruction.

DD Howell stated that the current set up for wiping drives was not conducive to ensuring a proper chain of custody of evidence, since 15 different technicians shared the workroom. He would want to ensure that, if he were the technician completing the wiping process, he could be assured that the drive he left there to wipe from the day before was the same one that was still there the next day. He stated that the CSD would need to improve its physical storage capability if it planned to maintain a strict chain of custody of the EDSCs.

He stated that the CSD currently only provided services for computer related issues and limited Blackberry support. He confirmed that the only wiping currently done for the Blackberry was carried out using the wiping feature provided on the device itself. He stated that the Blackberry wiping feature was DOD certified, but admitted that he did not know what level of wiping that function actually provided. DD Howell also noted that not all Blackberries were brought to the CSD when taken out of service.

The CSD does not currently provide any support services for EDSCs such as the ones contained in photocopiers, fax machines, CDs, DVDs, jump drives, or any other memory devices other than computers and Blackberries.

7.11.5 Classification of data

DD Howell highlighted during the meeting on 19 February that one of the primary obstacles faced by the CSD is that information within government is

not designated a security classification. This means that, when a machine is earmarked for wiping or destroying, the Department has no way of knowing how sensitive the information on the computers might be. Therefore, the only way to appropriately address the securing of information that may remain on the hard drives would be to completely destroy the hard drive.

DD Howell noted that in cases where there was highly classified information that needed to be protected, a hard drive should be degaussed and then physically destroyed. When this action was taken, a hard drive was rendered unusable. DD Howell believed that this would be a heavy-handed approach, as he was not aware of any information within government that would require such high security.

DD Howell estimated that the cost involved in going to this extreme would be the cost of the degausser and the cost of the hard drives that would be destroyed that could potentially be used elsewhere. He stated that a degausser would cost approximately $15,000. In his opinion, this would be "overkill", as many of the hard drives did not contain data relating to, say, national security. Rather than destroying them, he suggested the machines could be re-imaged and used as spares or wiped and then used for civil servants to buy for home use, or provided to various charities.

The issue of classification was also discussed in the response of the Director of the Information & Communication Technology Authority ("ICTA"), Mr. David Archbold, and was said to be an issue that had long been worthy of attention.

DD Howell stated that in light of the OCC investigation, the CSD had moved to treating all containers as if they contained highly classified (e.g., secret or top secret) information. They would be destroying all hard drives given to them for disposal until a standard could be set that was acceptable for the current general data classification of government documents.

DD Howell felt that greater attention needed to be placed on the classification of documentation if disposal policies were going to be cost effective. If the CSD took the disposal of EDSCs to the ultimate level of security, he stated, then the Department would be destroying hard drives that could potentially be of use in some other computer within or outside government.

7.11.6 Clarity of service requested and provided

The OCC seized a computer from CINA that had recently been wiped by the CSD. A CINA staff member said that she had received the computer from a CSD technician after it had been worked on by the CSD, and was told that the computer had been "wiped". The Director of CINA was also under the impression that the CSD had removed the information that had previously been on the machine.

The OCC had the computer tested and, with the help of specialist software, was able to find a great number of files, including many personal emails, memos, reports, etc. that were still on the hard drive.

Contact was made on 4 March 2009 with the CSD's DD Whittaker, who subsequently provided documentation from the CSD Computer Helpdesk log, as well as a statement from the technician who performed the work on that computer. The evidence provided was insufficient to make a clear determination as to what work had been requested by CINA, but the CSD, prior to being informed by the OCC what was found on the computer, stated that the machine in question had never been wiped. DD Whittaker stated that the machine had not been recommended for condemnation and the CSD understood that the machine was to be returned to CINA and was therefore only re-imaged.

In this instance, the communication and documentation between the CSD and CINA was insufficient to determine any fault. It is also important to note that CINA, while it intended to remove this computer from its asset registry, and was under the impression that the machine had been wiped by the CSD, did not intend to discard the computer at this time.

8. Overall Summary of Findings

1. None of the Portfolios and Ministries investigated had a policy for addressing the disposal of EDSCs. It was also determined that none of the Ministries and Portfolios had sufficient procedures to demonstrate that they were properly managing and disposing of EDSCs.

2. With the exception of the Department of Tourism under the Ministry of Tourism and the Department of Education under the Ministry of Education, which have their own internal IT support functions for limited areas, all the Ministries and Portfolios claimed that they and their respective departments relied on the CSD to provide for the disposal of IT equipment including Blackberries when and if the need arose.

3. There was an overall lack of adequate documentation of EDSC disposal throughout the Ministries and Portfolios as well as at the CSD.

4. There was a general lack of awareness on the part of COs as to what should be done with EDSCs, as well as what was ultimately being done with EDSCs. Most of them were aware of their procedure for removing of the actual asset from their asset registry, but once that process was completed there was no corporate memory and no further paper trail that could sufficiently verify what had happened to the EDSCs.

5. Until the launch of this investigation, the CSD would provide disposal services to any government department that requested this service. Once the computer had been properly removed from an entity's asset registry, the CSD would assess whether any parts could be salvaged for spare parts. This process included saving the hard drives if they could be used in other machines. These hard drives, if kept, were re-imaged. They would only be wiped if that process had been specifically requested by the entity. Once the computer had been stripped of any useful parts, the CSD would then take the remaining equipment to the landfill. While the CSD indicated that these machines were crushed, there was no way to verify if in fact that was being done. In the past, the CSD would only use a sledgehammer to smash hard drives deemed to be of no useful purpose.

6. It was apparent that communication between departments and CSD was not precise and that terminology was not used consistently. This may have resulted in a particular department seeking a higher level of service than was actually provided by the CSD.

7. This investigation revealed that COs were failing to take responsibility for adequately documenting and tracking the secure disposal of EDSCs. It appeared that the COs only ensured that assets were removed from the asset registries.

8. Data classification should be done, and be part of recycling and destruction process.

9. COs have not properly addressed the issue of the removal of government data once placed on civil servants' private computers.

9. Analysis

The lack of adequate documentation of EDSC disposal made it impossible to verify what equipment and how much equipment had been destroyed, as opposed to having been placed in a department storage container, given to a charity, sold to a member of staff, or thrown away in a dumpster.

The statement by CO Mr. Donovan Ebanks that a number of computers from his Portfolio had at one time been donated to the prison's educational program (and could not be verified as having been wiped), as well as the case of the private local charity that received computers from another government entity that still contained government files, led to the conclusion that some EDSCs have been released from the possession of the government and that all of them were not disposed of in a manner that ensured that the data was rendered inaccessible. The evidence of a lack of policy and procedure also led to the conclusion that, were it not for this investigation bringing the matter to the attention of COs, many other EDSCs would have been disposed of without ensuring that the data on them was rendered inaccessible.

It was clear that none of the Portfolios and Ministries were maintaining records of the use and ultimate disposal of EDSCs. The only records produced at the Portfolio/Ministry level related to the general disposal of the traditional physical assets. Ultimate responsibility for the tracking of the actual disposal of the EDSC was passed on to the CSD. While the CSD was able to provide some information regarding the assets that it had collected from the various departments, it did not have any record of what then happened to the EDSCs. Evidence from the CSD staff members exposed confusion and a lack of consensus on appropriate standards and procedures.

While the CSD potentially has the expertise to advise government on the recommended procedures for disposing of EDSCs, and in many instances may be the body requested to provide the service of disposal, the responsibility to ensure that EDSCs are adequately tracked through to final disposal rests with the COs. One option is that the CSD could provide a specific report, which could be attached to the CO's disposal record, outlining what exactly was done with each EDSC and related computer equipment.

The creation and implementation of a data classification system remains a project that should be completed. The failure to classify data and the resulting inability to know the level of care to be taken in decommissioning an EDSC impairs the design of an efficient and cost effective recycling and disposal process.

The use of personal computers and their retention of government information was an issue that was beyond the technical expertise of many of the COs interviewed. It is appropriate, then, to emphasize the need for this issue to be addressed while policy is developed. While it is true that the data transferred to a personal computer is still owed by government, and covered by confidentiality undertakings provided by government employees, arrangements must still be made for its proper disposal.

10. Conclusion

This own motion investigation by the OCC found that COs were not adequately tracking the use and disposal of EDSCs within their respective Ministries/Portfolios. Until the launch of this investigation by the OCC, very little attention had been given to the issue of secure disposal of EDSCs. It was clear that COs were unaware of what was being done with the EDSCs being disposed of from their Ministries/Portfolios and the departments under them.

While it has also become clear that not all EDSCs pose significant risk to the security of sensitive information, there is no way of clearly identifying which ones could pose a serious risk as information has not been classified. Regardless of what EDSCs are being considered, and regardless of what

information is being stored on these containers, the process of tracking and monitoring the disposal of these containers has been insufficient to ensure that EDSCs are being disposed of properly.

As the COs have the responsibility of overseeing the assets of their Portfolio/Ministry as well as ensuring that records are being securely maintained, each Portfolio/Ministry must have a policy that provides for the secure maintenance and disposal of all EDSCs. However, the policy required for such a process need not be specifically designed to be unique to each Portfolio/Ministry and it is likely best that there be one policy developed for all of the public sector. The expertise required for the development of the policy potentially could come from the CSD, CINA and existing published works from abroad. It would be appropriate for the Chief Secretary to take oversight of this project. However, no objection would be raised if the issues were addressed as part of the current process to amend the Financial Regulations under the direction of the Financial Secretary.

What is a proper policy for the disposal of EDSCs? The new policy and procedures must protect private and sensitive information to a degree that is commensurate with the risk of, and the damage caused by, unauthorized publication. It must include appropriate documentation that provides an auditable record trail from the introduction of the EDSCs into the government through to their final disposal, including appropriate evidence of what happens to the EDSC as it leaves government whether by donation to outside agencies, sale to individuals, or destruction. Responsibility for maintaining this paper trail falls to the COs. There are many well thought out policies available that could be referenced in the development of a policy for the Cayman Islands Government.

With the introduction of this enhanced practice of monitoring and secure disposal of EDSCs, there will be a need for all civil servants to be made aware of the importance of properly securing, maintaining, and disposing of all EDSCs.

11. Recommendations

It is recommended that:

1. Each Portfolio/Ministry have a policy on the use and proper disposal of EDSCs.
2. The policy for the use and proper disposal of EDSCs should be drafted in consultation with the CSD and CINA.
3. If a government entity does not use the CSD as its IT service provider, it must take steps to ensure that its service provider follows the new policy.

Office of the Complaints Commissioner
7 April 2009