AUDIT OF RECORDS
MANAGEMENT PROGRAM

JANUARY 27, 2015

PERFORMED BY:
DAVID J. AUBREY, CIA, CFE
ACTING INSPECTOR GENERAL
MEMORANDUM

TO: K. Mayock, Acting Corporate Secretary and Acting General Counsel
J. White, CFO
K. LaMarca, Director, IS

FROM: D. J. Aubrey

SUBJECT: Audit of Records Management Program

DATE: January 27, 2015

An audit of the Records Management Program was performed by David J. Aubrey, Acting Inspector General, Office of the Inspector General (OIG). The objectives of this audit were to evaluate the effectiveness of, and compliance with, Delaware River Port Authority (DRPA) and Port Authority Transit Corporation policies, procedures, and processes governing records management, retention, and destruction, and assess the management of the current Iron Mountain contract (off-site records storage) for compliance and billing accuracy. The audit scope included Authority-wide, local departmental, and external storage vendor policies, procedures, and processes for both DRPA and PATCO (both DRPA and PATCO hereafter referred to as “the Authority”). The assessment included both hard-copy and electronic media.

This audit was performed during June through December 2013. At the onset of this audit, the OIG emailed an internal control questionnaire / survey to the respective Chiefs within the Authority in an effort to obtain feedback regarding understanding of the records management program, policy, and perception of compliance. To assist in the evaluation of Authority’s Record Management Program, OIG requested and was provided access to the following information:

- Summary Statement and Resolution (SS&R) DRPA-12-044, dated April 18, 2012;
- Iron Mountain Contract (GN-0008-12), effective May 1, 2012 (and associated documents);
- Current and prior Record Retention Schedules (RRSs);
- Accounts Payable disbursement reports, invoices, Contract Voucher Form (associated with current Iron Mountain contract, covering the period May 2012 through April 2013 (paid October 2012 through May 2013); and,
- Iron Mountain information and tracking system reports (i.e. storage reports, destruction activity reports, shredding activity reports, etc.).
In addition to accessing the documentation noted, OIG performed on-site visits at Iron Mountain Inc.’s Malvern, PA and Sharon Hill, PA facilities. Meetings, discussions, correspondence with representatives from the Authority’s Office of the Corporate Secretary (OCS), Office of the General Counsel / Legal (OGC), Finance Department, as well as Iron Mountain Inc. representatives, also took place during the course of this audit.

Based on the testing performed, opportunities exist for enhancing the Authority’s Records Management Program and associated control environment. Due to the critical importance of the Authority’s Records Management Program and the number of issues encountered, a comprehensive audit report is presented touching upon key opportunities for improvements not only focusing on the Records Management Program, but other related processes encountered as well. In summary, the following significant opportunities for improvement were noted:

- The most recent RRSs were dated as prepared / revised during the year 2009. Some RRSs contained hand-written edits / changes that have not been incorporated on a final / approved RRS, indicative that records retention maintenance was not performed on a routine basis.
- Records stored off-site had not been destroyed even thought their noted retention period (supplied destruction date) had been passed. Efforts were made by the OCS and OGC to address destruction of records stored off-site and in excess of noted destruction dates during the course of this audit.
- Records Management compliance is not periodically reviewed by Records Management staff.
- OGC / Legal compliance is lacking based on the fact that the current RRSs did not include any observable indication / documentation of OGC / Legal review.
- There was an absence of guidance pertaining to the handling and retention of Authority e-mail and other mediums used to store records / documents.
- A potential opportunity for savings is available if the Authority shifts the process for the shredding of documents within secured containers from on-site shredding (“secured”) to off-site shredding (“standard”).
- Records Management RBase database has not been accessed by the Administration Coordinator to edit existing RRSs and create new RRSs since assuming the records management responsibilities.
- Review of RRSs identified: inconsistent record naming convention, inconsistent retention periods applied to identically named records and similar records / record series, key records were not noted on RRSs of logical responsible area, and, a need for guidance as to what should be included / retained within a set of records.
- Pricing schedule(s) included within the Iron Mountain contract documentation provided to OIG did not reflect all prices invoiced. Additional pricing schedules were provided directly to the Administrative Coordinator from Iron Mountain and were not reviewed / approved by the Manager, Contract Administration, nor the former Corporate Secretary / General Counsel.
- Documentation supporting the unsuccessful competitor’s original quote and the associated bid evaluation to support the awarding of the contract could not be located by Contract Administration.
• A detailed invoice approval process (i.e. comparing service activity / volume reported and the associated contracted billing rate) was not performed. The invoices were reviewed for reasonableness only.

• Storage services / activity associated with the PATCO account (PE089) for the month of January 2013, valued at $404.46, were invoiced by Iron Mountain and paid by the Authority twice.

• DRPA Accounts Payable was not aware, nor informed, that PATCO related storage charges were being applied to DRPA’s account since the inception of the new agreement with Iron Mountain and the subsequent invoicing of PATCO storage activity. PATCO charges were being incurred and paid by DRPA and were not being charged back to PATCO accounts. Since this was identified in its early stages, PATCO charges incurred by DRPA totaled $3,075.

• Authority records stored in Iron Mountain’s “climate controlled” vault may not need the additional protection / security and environment provided. Savings can be achieved by shifting the contents to Iron Mountain’s traditional, standard storage option currently in use for the majority of the Authority’s records stored off-site.

• The former Corporate Secretary / General Counsel did not have authorization to access Iron Mountain’s web-based system, nor authorize / approve the destruction of any Authority electronic back-up files in storage. The Director, IS, a Systems Administrator, and the Administrative Coordinator have full web-based access, rights, and authority to make changes to this account, including requesting media destruction.

• The Authority’s Record Management Program procedure does not include guidance regarding when and if scanned copies of documents are acceptable as documents of record.

• According to the Director, IS, the most recent disaster recovery exercise was undertaken during November 2011. A formal written Disaster Recovery report has not been written by the Authority’s Information Services Department. The results of the most recent Disaster Recovery exercise have not been shared with the Authority’s executive management, or the Board of Commissioners.

• The Authority’s Computer Disaster Recovery policy outlines “management” responsibilities associated with Disaster Recovery (including Back-up); however, accountability is not clearly defined, the back-up policy is not defined (systems/programs/records/data, frequency, retention, etc.), and steps to achieve system recovery are not detailed. The policy does not formally address: 1) definition of the frequency of recovery testing beyond the term “regularly”, 2) internal documentation requirements relating to the testing scope, performance, and results, and 3) formal reporting requirements to executive management and the Board of Commissioners.

• The Authority’s off-site storage facility is not visited to physically verify back-up files in storage, assure adequacy of facility, determine compliance with contracted terms, and observe physical security / environmental control practices.

• Formal Records Management training and readily accessible guidance is not apparent.
These issues, together with the others identified during our audit, were reviewed with the responsible Authority management, who has subsequently resolved some of the identified issues and, established a time line to implement corrective actions for the remaining open issues. Details of the audit are included within the attached report. During the conclusion of this audit the Corporate Secretary / General Counsel resigned; however, the current Acting Corporate Secretary / General Counsel is supportive of the management responses included within the attached report. According to the Acting Corporate Secretary / General Counsel, the resolution of the majority of issues and recommendations reported within this audit are contingent upon the Authority hiring a Records Manager. The associated hiring process is currently in progress.

OIG wishes to thank the management and personnel who participated in this audit for their cooperation during the engagement.

cc: E. DePasquale, Chairman, Board of Commissioners
J. Nash, Vice Chairman, Board of Commissioners
R. Taylor, Vice Chairman, Audit Committee
J. Hanson, CEO
Table of Contents

A. Objective / Scope / Methodology .................................................................................................... 1
B. Background ..................................................................................................................................... 1
C. Audit Summary ............................................................................................................................. 3
D. Policy / Procedure / Process Analysis ........................................................................................... 5
E. Records Retention Schedule Review .......................................................................................... 11
F. Procurement Process .................................................................................................................... 16
G. Invoice Review ........................................................................................................................... 23
H. Iron Mountain On-site Visits ........................................................................................................ 25
I. Information Services – Backup and Recovery .............................................................................. 31
J. Training / Communication ........................................................................................................... 35
K. Internal Control Questionnaire Summary (See Attachment A) ..................................................... 36
A. Objective / Scope / Methodology

The objectives of this audit were to evaluate the effectiveness of, and compliance with, Delaware River Port Authority (DRPA) and Port Authority Transit Corporation (PATCO) policies, procedures, and processes governing records management, retention, and destruction, and assess the management of the current Iron Mountain contract (off-site records storage) for compliance and billing accuracy.

The audit scope included Authority-wide, local departmental, and external storage vendor policies, procedures, and processes for both DRPA and PATCO (both DRPA and PATCO hereafter referred to as “the Authority”). The assessment included both hard-copy and electronic media.

This audit was performed during June through December 2013. At the onset of this audit, the Office of the Inspector General (OIG) emailed an internal control questionnaire / survey to the respective Chiefs within the Authority in an effort to obtain feedback regarding understanding of the records management program, policy, and perception of compliance. To assist in the evaluation of Authority’s Record Management Program, OIG requested and was provided access to the following information:

- Summary Statement and Resolution (SS&R) DRPA-12-044, dated April 18, 2012;
- Iron Mountain Contract (GN-0008-12), effective May 1, 2012 (and associated documents);
- Current and prior Record Retention Schedules (RRSs);
- Accounts Payable disbursement reports, invoices, Contract Voucher Form (associated with current Iron Mountain contract, covering the period May 2012 through April 2013 (paid October 2012 through May 2013); and,
- Iron Mountain information and tracking system reports (i.e. storage reports, destruction activity reports, shredding activity reports, etc.).

In addition to accessing the documentation noted, OIG performed on-site visits at Iron Mountain Inc.’s Malvern, PA and Sharon Hill, PA facilities. Meetings, discussions, correspondence with representatives from the Authority’s Office of the Corporate Secretary (OCS), Office of the General Counsel / Legal (OGC), Finance Department, as well as Iron Mountain Inc. representatives, also took place during the course of this audit.

B. Background

Records retention schedules serve as an organization’s legal authority to retain and purge records, and, as a result, hold great importance for an organization. It is a goal of a records retention schedule to capture all of the types of records created and used by an organization in the execution of its business, and indicates how long these records are required to be retained. A retention schedule needs to be developed and applied in an orderly method, as part of an organization’s corporate-wide records management strategy. The development and implementation of a retention schedule are important
elements in establishing a "good faith" effort, and ensuring a complete and reliable records management program.

As the capacity of retained business records expands, so does the risk of not having a retention schedule. The absence of retention schedules may result in increased litigation exposure through retaining records longer than legally necessary and/or delayed response and inaccuracies to discovery requests and regulatory inquiries.

Establishing how long to retain records requires the development and implementation of a credible records retention policy. Irregularity or inconsistency in an organization’s records program, or the absence of a credible records management program, can negatively affect internal and external stakeholder’s assumptions of good faith. Lacking a viable reason, keeping records for longer or shorter times than approved published guidelines dictate exposes a company to unnecessary reputational and legal risk.1

According to Summary Statement and Resolution (SS&R) DRPA-12-044, dated April 18, 2012, the DRPA has utilized an off-site records storage provider beginning prior to year 2002 based upon the advice of a Records Retention consultant engaged by DRPA. After some difficulties with a prior off-site storage provider, DRPA determined to use Iron Mountain Information Management, Inc. (Iron Mountain). The initial Iron Mountain contract was executed in year 2004. Thereafter Iron Mountain was able to offer DRPA its services pursuant to a General Service Agreement (GSA) and DRPA participated under the GSA contract and rates. The GSA standards changed, and as a result Iron Mountain would have had to move all GSA contract customers including DRPA to a facility in Virginia. After analyzing the changes in the GSA requirements, DRPA needs, and the increased costs and time requirements, DRPA reverted to a non GSA contract with Iron Mountain.

DRPA -12-044 authorized the current contract with Iron Mountain (GN-0008-12), effective May 1, 2012, with a 5 year total value not to exceed $200,000 (Maximum Fee).

During the late 1990’s, the Authority hired a records retention consultant for the purpose of establishing an effective records management program and assist in the procurement of effective off-site storage services (including an off-site storage facility). The records management program was initially established within the responsibility of what was then called Administrative Services, and included the creation of approved record retention schedules, policies and procedures, as well as training material. As a result of organizational changes within the Authority, the responsibility for oversight and maintenance of the Authority’s records management was transferred to, and currently resides under, the charge of the OCS.

1 http://www.acc.com/legalresources/quickcounsel/rr.cfm#theimp
C. Audit Summary

Based on the testing performed, opportunities exist for enhancing the Authority’s Records Management Program and associated control environment. Due to the critical importance of the Authority’s Records Management Program and the number of issues encountered, a comprehensive audit report is presented touching upon key opportunities for improvements not only focusing on the Records Management Program, but other related processes encountered as well. In summary, the following significant opportunities for improvement were noted:

- The most recent RRSs were dated as prepared / revised during the year 2009. Some RRSs contained hand-written edits / changes that have not been incorporated on a final / approved RRS, indicative that records retention maintenance was not performed on a routine basis.
- Records stored off-site had not been destroyed even though their noted retention period (supplied destruction date) had been passed. Efforts were made by the OCS and OGC to address destruction of records stored off-site and in excess of noted destruction dates during the course of this audit.
- Records Management compliance is not periodically reviewed by Records Management staff.
- OGC / Legal compliance is lacking based on the fact that the current RRSs did not include any observable indication / documentation of OGC / Legal review.
- There was an absence of guidance pertaining to the handling and retention of Authority e-mail and other mediums used to store records / documents.
- A potential opportunity for savings is available if the Authority shifts the process for the shredding of documents within secured containers from on-site shredding (“secured”) to off-site shredding (“standard”)
- Records Management RBase database has not been accessed by the Administration Coordinator to edit existing RRSs and create new RRSs since assuming the records management responsibilities.
- Review of RRSs identified: inconsistent record naming convention, inconsistent retention periods applied to identically named records and similar records / record series, key records were not noted on RRSs of logical responsible area, and, a need for guidance as to what should be included / retained within a set of records.
- There are no controls in place to readily assure that all executed contracts / agreements are on file.
- There is no guidance as to what contracts / agreements the OCS is accountable for retaining, nor the level of documentation supporting the associated procurement process (i.e. authorized contract/agreement, authorized SSR, RFP-Request for Procurement, RFQ-Request for Quotation, associated vendor quotations / bids, contract award analysis and award justification, etc.).
- Pricing schedule(s) included within the Iron Mountain contract documentation provided to OIG did not reflect all prices invoiced. Additional pricing schedules were provided directly to the Administrative Coordinator from Iron Mountain and were not reviewed / approved by the Manager, Contract Administration, nor the former Corporate Secretary / General Counsel.
- Documentation supporting the unsuccessful competitor’s quote and the associated bid evaluation to support the awarding of the contract could not be located, and was not supplied, by Contract Administration.
• National Archives and Records Administration (NARA) standards require research as to the applicability of the compliance requirements relating to the Authority’s off-site records storage activity.
• A detailed invoice approval process (i.e. comparing service activity / volume reported and the associated contracted billing rate) was not performed. The invoices were reviewed for reasonableness only.
• Storage services / activity associated with the PATCO account (PE089) for the month of January 2013, valued at $404.46, were invoiced by Iron Mountain and paid by the Authority twice.
• DRPA Accounts Payable was not aware, nor informed, that PATCO related storage charges were being applied to DRPA’s account since the inception of the new agreement with Iron Mountain and the subsequent invoicing of PATCO storage activity. PATCO charges were being incurred and paid by DRPA and were not being charged back to PATCO accounts. Since this was identified in its early stages, PATCO charges incurred by DRPA totaled $3,075.
• Authority records stored in Iron Mountain’s “climate controlled” vault may not need the additional protection / security and environment provided. Savings can be achieved by shifting the contents to Iron Mountain’s traditional, standard storage option currently in use for the majority of the Authority’s records stored off-site.
• The former Corporate Secretary / General Counsel did not have authorization to access Iron Mountain’s web-based system, nor authorize / approve the destruction of any Authority electronic back-up files in storage. The Director, IS, a Systems Administrator, and the Administrative Coordinator have full web-based access, rights, and authority to make changes to this account, including requesting media destruction.
• The Authority’s Record Management Program procedure does not include guidance regarding when and if scanned copies of documents are acceptable as documents of record.
• According to the Director, Information Services (IS), the most recent disaster recovery exercise was undertaken during November 2011. A formal written Disaster Recovery report has not been written by the Authority’s IS Department.
• The results of the most recent Disaster Recovery exercise have not been shared with the Authority’s executive management, or the Board of Commissioners.
• The Authority’s Computer Disaster Recovery policy outlines “management” responsibilities associated with Disaster Recovery (including Back-up); however, accountability is not clearly defined, the back-up policy is not defined (systems/programs/records/data, frequency, retention, etc.), and steps to achieve system recovery are not detailed. The policy does not formally address: 1) definition of the frequency of recovery testing beyond the term “regularly”, 2) internal documentation requirements relating to the testing scope, performance, and results, and 3) formal reporting requirements to executive management and the Board of Commissioners.
• IS had not interacted with the third party data back-up storage facility (Iron Mountain) in the performance of the most recent disaster recovery testing.
• The Authority’s off-site storage facility is not visited to physically verify back-up files in storage, assure adequacy of facility, determine compliance with contracted terms, and observe physical security / environmental control practices.
• Formal Records Management training and readily accessible guidance is not apparent.

These summarized issues, as well as others, are presented in more detail within the audit report, along with recommendations and management’s responses / corrective actions.
D. Policy / Procedure / Process Analysis

DRPA / PATCO Policies and Procedure Manual Series 212 Records Management Program dated March 15, 2000 and revised December 8, 2006 governs the Authority’s Record Management Program which covers all records, in all formats, throughout their useful life cycle, created, received, managed and retained by the Authority. All Authority departments are required to comply with the Records Management policy. This policy defines broad areas of responsibility / accountability; specific detailed procedures / guidelines were not provided. [OIG did find guidance buried within the DRPA’s intranet (E.NET) files, a Records Management Training Manual related to the initial launching of DRPA’s Record Management Program. This training manual was noted as associated with the now non-existent Administrative Services Division. The referenced training manual will be further addressed within Section J – Training / Communication.] Key responsibilities highlighted within the Authority’s policy include:

- Retention Schedules: each business or financial unit shall maintain a current and complete RRS.
- Records Retention: all records must be kept for full retention period.
- Records Management Procedures: each responsible area shall ensure all records retained on-site or off-site are properly identified and maintained to assure accurate / prompt retrieval.
- Purging of On-site Records: Corporate Secretary will schedule an annual purging of on-site records.
- Record Retention Maintenance: RRS will be reviewed annually by the Departments (Legal, Finance, etc.) to be updated to reflect significant org changes, changes in responsibilities, and / or type of records retained. Corporate Secretary will coordinate and send notice of review dates to all Departments.
- Vital Records: Each responsible area will adhere to practices protecting information vital to it continuing operations in the event of disaster.
- Records Management Program Compliance: each DRPA and PATCO department shall be periodically visited by a member of the Authority’s Records management staff to determine compliance with record management procedure.
- OGC Responsibilities: Legal is responsible for reviewing all Record Retention Schedules (RRS) to assure all legal, statutory, and regulatory requirements are met, providing legal advice regarding record retention; and issuing destruction hold orders when necessary.

Key levels of responsibility and accountability noted within the Authority’s policy include:

- OCS: responsible for operation of the Authority’s Records Management Program, monitor compliance of records management policies and procedures, with management to assure compliance.
- Legal Department (OGC): review retention schedules to assure all legal, statutory, and regulatory requirements are met; provide legal advice with respect to record keeping and
retention issues; issues destruction hold orders when it is necessary to retain records beyond their scheduled retention periods.

- **Department Management:** responsible to ensure that the Records Management Program is fully implemented in their areas, in compliance with the Authority’s policies and procedures; to appoint records coordinators (records management representative) for their areas.

- **Security and Business Continuity Administrator:** work with Corporate Secretary to ensure that an appropriate protection strategy has been implemented for each vital records series.

**Audit Finding 1:** Records Management Program policy compliance was discussed with the former Corporate Secretary / General Counsel, and the Administrative Coordinator to the Corporate Secretary (Administrative Coordinator). Based on those discussions, OIG determined the following regarding key policy driven control responsibilities:

- The most recent RRSs were dated as prepared / revised during the year 2009; some RRSs contained hand-written edits / changes that have not been incorporated on a final / approved RRS. This was also indicative that Records Retention maintenance was not performed on a routine basis.

- Regarding Records Retention compliance, records stored off-site had not been destroyed even though their noted retention period (supplied destruction date) had been passed. Based on discussion with the OCS and OGC, efforts were made to address destruction of records stored off-site and in excess of noted destruction dates during the course of this audit. Records maintain on-site within the Authority’s office buildings are subject to retention compliance enforced by the respective local management and based on their respective RRS.

- Annual on-site purging of records on file at the Authority was last announced during March 2012, and performed during April 2012. This was coordinated by the Authority’s Chief Operating Officer, but should have also involved the Corporate Secretary / General Counsel for compliance oversight (... the involvement of the former Corporate Secretary / General Counsel was not readily apparent based on the recipients of the emailed correspondence ). The goal of this event was to purge old records maintained at the Authority. The emailed communication noted to follow standard operating procedure associated with DRPA recordkeeping, and if uncertain to “ask before you trash”.

- The definition of “Vital” records needs to be effectively defined and communicated to those responsible for ensuring they are properly identified and retained. There were not many “Vital” records noted on the RRSs reviewed. According to the Authority’s Records Management Program policy, the following reference is provided: “Vital Records: Each unit shall adhere to practices to protect information vital to its continuing operation in the event of a disaster”. According to the “Records Management Training Manual” buried in the Authority’s intranet, “A vital record is one that would enable Delaware River Port Authority to recreate its legal and financial status and meet its obligations to clients and employees after a major catastrophe. Only a small percentage of the records are classified as vital”. Based on OIG’s discussions resulting from internal
control questionnaire / survey responses, one area was unaware of the definition for a “Vital” record classification; also, those overseeing the records management process were not familiar with the “Vital” record definition / criteria.

- Records Management compliance is not periodically reviewed by Records Management staff. The only dedicated Records Management staff includes the Administrative Coordinator, who includes her records management responsibilities along with her other Authority based duties (including Authority Board meeting coordination and support).

- OGC compliance is lacking based on the fact that the current RRSs (created during year 2009) did not include any observable indication / documentation of OGC review. The Administrative Coordinator confirmed that there was no OGC review of the most recent RRSs (ddt 2009). The most current RRSs with an OGC approval that were provided to and observed by OIG were created in the year 2006.

- The policy references a “Security and Business Continuity Administrator”, this specific position or assigned responsibility, was not apparent or identified.

**Audit Recommendation 1.1:** The Corporate Secretary / General Counsel should inventory the current RRSs to assure all responsible areas within the Authority are represented. RRSs should be updated to reflect any organizational changes, changes in responsibilities, and the impact on these changes to respective records / document handling. RRSs should be evaluated to assure all key records / record classes are reflected for each responsible area. The new RRSs, in compliance with Authority policy, should be appropriately reviewed and signed-off / authorized by the responsible area’s management and OGC (documenting formal review and approval of records and retention periods). A retention schedule and policy should be viewed as dynamic. The retention schedule should be reviewed periodically (approximately every 18 to 24 months) to determine the impact of any organizational / legal changes upon records retained and their retention periods.

**Management’s Response 1.1:** The Acting Corporate Secretary / Acting General Counsel agrees with the recommendation and the critical need of hiring a professional records retention individual for providing “best practices” guidance and/or continued effective management of the records management function. The hiring of a Records Manager had been previously requested by the former Corporate Secretary / General Counsel. Interviews for the Records Manager role had previously been conducted; however, candidates did not meet minimum qualifications. Subsequent delays associated with the reposting of this position, and the related hiring process, have precluded the position from being filled. The Records Manager position was communicated by Human Resources to Authority employees by Authority email, posted online to the Authority website, and qualified applicants were requested (email issued by Human Resources September 15, 2014). The associated interview process, which had been suspended, has recently resumed. Once this position has been filled, the recommended corrective actions within this audit report will be addressed as part of the new Records
Manager’s responsibilities. The Acting Corporate Secretary / Acting General Counsel believes the use of a consultant should also be considered on the review and updating of the existing RRSs and the associated RRS process.

Audit Recommendation 1.2: The Corporate Secretary / General Counsel should institute an annual records review/purge in accordance with established policy, providing the Authority with the proper level of guidance as to what documents / records can and should be destroyed.

Management’s Response 1.2: The former Corporate Secretary / General Counsel agreed with the recommendations; however, additional staffing resources are required to effectively implement the recommended actions. The implementation of the corrective actions to address this recommendation will be undertaken as part of the responsibilities of the new Records Manager upon their hire. (See Management Response 1.1)

Audit Recommendation 1.3: The Corporate Secretary / General Counsel should define a “Vital” record (with key examples) and communicate this information to the Authority to assure records of this nature are captured on the Authority’s RRSs and retained for future reference (if needed).

Management’s Response 1.3: The former Corporate Secretary / General Counsel agreed with the recommendations, and believed this definition that should be created by and provided under the responsibility of the General Counsel, OGC. The responsibility for implementation of this recommendation will be assigned to the new Records Manager upon their hire. (See Management Response 1.1)

Audit Recommendation 1.4: The Corporate Secretary / General Counsel should determine the need for a “Security and Business Continuity Administrator”, and revise the Authority’s Records Management policy based on that decision.

Management’s Response 1.4: The former Corporate Secretary / General Counsel agreed with the issue and recommendation, and was not aware of anyone serving in the capacity of “Security and Business Continuity Administrator”. While the former Corporate Secretary / General Counsel concurred with the issue and recommendation, she could not provide a realistic target date for implementation of corrective actions. The implementation of the corrective actions to address this recommendation will be undertaken via the creation and posting of a new position or the associated responsibilities will be absorbed as part of the job description for the new AGC upon their hire. This responsibility will be evaluated upon the hiring of the Records Manager, and the Authority’s Records Management policy will be revised accordingly. (See Management Response 1.1)
There was an absence of guidance pertaining to the handling and retention of Authority e-mail and other mediums used to store records / documents (i.e. portable computing devices - laptops, tablets, IPads, etc., portable / external electronic data storage devices - thumb drives, CDs, DVDs, hard drives, etc., and cellular / smart phones). This conclusion was supported by review of the Authority policy, as well as feedback received from the internal control questionnaire supplied to all areas of the Authority. With the proliferation of the use of e-mail as the correspondence method-of-choice, and the use of portable / hand-held devices, the reference of these areas and incorporation of associated guidance for handling of e-mail records within the Authority’s established records retention policy should be addressed.

**Audit Finding 2:** Absence of guidance pertaining to the handling and retention of Authority e-mail and other mediums used to store records / documents (i.e. portable computing devices - laptops, tablets, IPads, etc., portable / external electronic data storage devices - thumb drives, CDs, DVDs, hard drives, etc., and cellular / smart phones).

**Audit Recommendation 2:** The Corporate Secretary / General Counsel should revise the Authority’s Records Management policy, and create additional guidance, to address the handling and retention of Authority e-mail and other mediums used to store records / documents (i.e. portable computing devices - laptops, tablets, IPads, etc., portable / external electronic data storage devices - thumb drives, CDs, DVDs, hard drives, etc., and cellular / smart phones).

**Management’s Response 2:** The former Corporate Secretary / General Counsel agreed that the Authority’s Records Management policy should be revised to include guidance pertaining to the retention of emails and other electronically stored information. This recommendation shall be implemented after the hiring of the Records Manager and / or review and recommendations by a professional records management services company.

**Record Destruction Activity:**

OIG requested a summary of destruction activity associated with the DRPA’s Iron Mountain contract from contract inception (May 2012) through August 2013 from Iron Mountain. According to Iron Mountain there were two (2) destruction requests during this time period, but both had been cancelled. Since contract inception through August 2013, there was no record of destruction activity at Iron Mountain. Iron Mountain management informed OIG that the last requested destruction of Authority records in storage at their facilities was received in January 2011; subsequent record destruction was performed in April 2011. The absence of routine and prescribed destruction activity was communicated to OGC management during the course of the audit. Failure to destroy records which have reached and/or exceeded their respective retention periods increases the Authority’s litigation exposure and contributes to additional, unnecessary cost for storing the records. OGC management reviewed the records retained in off-site storage (Iron Mountain’s Sharon Hill facility) which were noted as exceeding their retention period. After their review, OGC management instructed Iron Mountain to destroy...
identified records that exceeded their retention periods and were not directly related to current litigation activity. Record destruction is scheduled and performed off-site from Iron Mountain’s Sharon Hill facility; certification of destruction is supplied by Iron Mountain after the documents are destroyed. Only documents that are stored at Iron Mountain’s off-site facilities (not including IT back-up files) are subject to authorization by the Corporate Secretary / General Counsel prior to destruction.

**Audit Finding 3:** Failure to destroy records which have reached and/or exceeded their respective retention periods, which can increase the Authority’s litigation exposure and contribute to additional, unnecessary cost for storing the records.

**Audit Recommendation 3:** The Corporate Secretary / General Counsel should assure that records stored off-site that have exceeded their established / approved retention periods are routinely destroyed, unless there is a litigation hold in place requiring the preservation of specified records / documents. At a minimum, documentation supporting the records authorized for destruction, authorization instructions, and a destruction certificate(s) should be retained as evidence of the records destruction process.

**Management’s Response 3:** The former Corporate Secretary / General Counsel agreed with the recommendation in respect to Authority documents, both electronic and hardcopy, which are currently in storage. The former Corporate Secretary / General Counsel, starting with the OGC management review which occurred during the course of the audit, had effectively addressed the routine and timely destruction of Authority records stored off-site that have exceeded their established / approved retention periods. Much of the content in storage that was reviewed by OGC was not documentation which should have been in offsite storage. The cancelled destruction orders were believed to be directly related to destruction holds associated with pending litigation activity. This oversight of the record destruction responsibility will be assigned to the new Records Manager upon their hire. Responsibility for approval of record destruction will continue to remain with the Corporate Secretary / General Counsel. According to Iron Mountain, destruction of 884.40 cubic feet of material was completed during February 2014, which will result in storage cost savings of approximately $2,160 / year.

**Shredding Activity:**

In addition to providing record storage and destruction services, Iron Mountain also provides on-site shredding services for the DRPA. The Administrative Coordinator periodically calls Iron Mountain to take the secured trash containers placed at various locations throughout the Authority and has the records within the containers shredded on-site. The Iron Mountain supplied trash containers are for the purpose of securing local, confidential records for eventual (near term) destruction. Since contract inception through August 2013, Iron Mountain visited Authority locations on 18 dates, associated with the shredding of records within 214 containers.
OIG noted a potential opportunity for savings. If the shredding services was not performed on-site (“secured”), but rather performed off-site (“standard”) at Iron Mountain’s facility, a savings of 20% could be realized ($15/container vs. $12/container). A Certificate of Destruction will be supplied by Iron Mountain (similar to the current “secured” approach to shredding).

Authority records that are locally destroyed (i.e. local shredders, documents placed in shredding containers, routine trash / recyclables, etc.) are not directly overseen, controlled, or authorized by the Administrative Coordinator, nor authorized by OGC. Records destroyed at this level are disposed of on a local, individual basis and subject to local supervision; however, the requirements of the area’s RRS should still be communicated and enforced. The Administrative Coordinator will periodically communicate with those who requested secured trash containers to determine if there is a need to request on-site shredding for their area.

**Audit Finding 4:** Potential opportunity for savings is available if the Authority shifts the process for the shredding of documents within secured containers from on-site shredding (“secured”) to off-site shredding (“standard”).

**Audit Recommendation 4:** The Corporate Secretary should evaluate the need to have Authority records shredded on-site by Iron Mountain. A cost saving of 20% can be realized if record shredding is performed at the Iron Mountain facility. Iron Mountain will provide a Certificate of Destruction for off-site records shredding, as they currently do for on-site shredding.

**Management’s Response 4:** The former Corporate Secretary / General Counsel agreed with the recommendation and agreed to implement the changes for routine pick-up of Authority documents within the secured trash containers throughout the Authority, and also allowing for the shredding of the associated documents to occur offsite at Iron Mountain’s shredding facility at a lower cost. The former Corporate Secretary / General Counsel agreed to implement these changes immediately and will notify OIG once put in place.

### E. Records Retention Schedule Review

Current Record Retention Schedules (RRS) supplied by OCS were not physically documented as approved by a representative of the Authority’s OGC, and in many cases, the operating management of areas associated with the RRSs did not sign off as well.

OIG requested the current RRSs for the Authority from the Administrative Coordinator. Based on OIGs review of the RRSs provided, the majority of schedules were dated as prepared / revised during the year 2009. All RRSs have designated sign-off requirements for the associated Department Head, as well as Finance, and OGC / Legal. Fifty percent of the schedules reviewed showed evidence of sign-off by the Department Head, but no schedule reflected evidence of sign-off by Finance or OGC / Legal indicating their review and approval. When discussed with the Administrative Coordinator, she commented that RRSs have not been reviewed by OGC / Legal, nor Finance. Forty-three RRSs were initially supplied by
the Administrative Coordinator, with an additional four being supplied later at OIG request. When requested, the OIG’s Record Retention Schedule could not be provided (nor the RRS of the former Internal Audit Department). The OIG is working with the OCS to develop a current RRS for the OIG. OIG could not be provided with any assurance that the entire Authority was represented within the schedules provided by the OCS – organizational changes, and changes to responsibilities since 2006 may have caused a need to realign and reassigned recordkeeping responsibilities.

RRSs were supplied to OIG that reflected local area management’s hand written notes for edit / change; updated versions of the RRSs, incorporating the edits / changes, were not provided.

When provided with a Records Management Manual, OIG located previous versions of RRSs that were developed in 2006. These schedules were noted as signed-off by the respective Department Heads, as well as OGC / Legal. There has been no other review and documented approval of the Authority’s RRSs by OGC / Legal since 2006.

OIG was informed of a Records Management RBase Database implemented by a hired Records Management Consultant (Noremco Services, Inc.), for the purpose of creating and maintaining the Authority’s RRSs. OIG was also informed that this database has not been accessed by the Administrative Coordinator in order to edit existing RRSs and create new RRSs since assuming the records management responsibilities.

**Audit Finding 5:** Records Management RBase database has not been accessed by the Administrative Coordinator to edit existing RRSs and create new RRSs since assuming the records management responsibilities.

**Audit Recommendation 5:** The Corporate Secretary / General Counsel should determine the value of the RBase database to facilitate the RRSs creation and maintenance requirements for the Authority’s Record Management program. If deemed adequate, those involved with administering the Records Management program should be familiar with / trained on the capabilities of the RBase database. If deemed unacceptable to address the current and future requirements of the Records Management program, a new records management system should be explored.

**Management’s Response 5:** The former Corporate Secretary / General Counsel agreed with the recommendation. The OCS has been reviewing and discussing optional systems; unfortunately, issues with staffing and failure to hire, has delayed this process. The implementation of the corrective actions to address this recommendation will be undertaken as part of the responsibilities of the new Records Manager upon their hire. (See Management Response 1.1)

OIG selected a sample of common key records / record series (or grouping of commonly named / similar records) from the current RRSs provided by the Administrative Coordinator. RRSs were reviewed to observe: 1) consistency in application of record naming convention, 2) consistency between the
sampled record names and their noted retention period, and 3) reflection of key records / record series on the RRSs of responsible areas where the key records / record series should have been included. The following was noted:

1) **Inconsistent record naming convention:** OIG reviewed the current RRSs and observed the use of inconsistent naming conventions when identifying records / record series. To insure a consistent application of the records management policy and retention / destruction periods, consistency must also be applied across the Authority when naming and identifying common records / record series. For example, the following similar classification of records have been named:

- Project Files, Project Files - Operational, Project File - Construction, Infrastructure, Capital Equipment, Project Files - Canadian Vickers Car Construction, Project Files - System Development / Conversion / Update;
- Correspondence Files, Correspondence - Incoming (PATCO), Correspondence - Outgoing (PATCO), General Correspondence,
- Subject Files, Administrative / Subject Files, Administrative Files, Subject Files - Transit Cars,
- Contracts/Agreements - Professional Services, Contacts/Agreements - Construction Contracts, Contacts/Agreements - Purchases / Professional, Contracts / Agreements, Agreements / Contracts / Agreements - Contracts - Advertising, Agreements / Contracts - Property Contracts / Indemnity Files, Agreements / Contracts - Construction / Professional Services, Agreements / Contracts - Maintenance and Service Contracts, Contracts / Agreements - Construction / Professional, Contract / Agreements - Procurement, Construction Contracts, Service Contracts, Intergovernment Contracts, and Contracts - State;
- Blanket Purchase Orders, Purchase Orders, Purchase Orders - Incomplete, Purchase Orders / Requisitions, Purchase Requisitions / Orders, Purchase Orders and RFPs, Purchase Requisitions, Request for Bids, Quotes.

2) **Inconsistent retention periods within identically named records and similar records / record series:** OIG reviewed the current RRSs and observed many instances where identically named records / record series had different retention periods noted on the RRSs; for example:

- Administrative Files: of the RRSs observed with this record, the majority reported this record as Current Year + 3, there were also instances of this record reported with a retention period of Current Year + 1 and Current Year + 2. Other similarly named record series has a retention period of Current Year + 3.
- Project Files - Operational: two RRSs reported this record with a retention period of Termination + 5, one schedule had a retention period of Termination + 2. Other similarly named record series had retention periods ranging from Termination +1 to Termination + 5.
- Subject Files: of the RRSs observed with this record, the majority reported this record as Current Year + 3, there were also instances of this record reported with a retention period of Current Year + 5 and Current Year + 6. In addition, some schedules included the symbol "H", requesting the responsible area to assure the record does not have any historical significance to the Authority prior to approving destruction. This was not consistently
denoted on all schedules. Another similarly named record had a retention period of Current Year + 3 or Superseded (w/ the "H" or historical reference noted).

- Correspondence Files: of the RRSs observed with this record, the majority reported this record as Current Year + 3, there were also instances of this record reported with a retention period of Current Year + 1, and one schedule reported a retention period of Current Year + 3. Other similarly named record series had retention periods ranging from Current Year +2 to Current Year + 3.

- Reference Files / Materials: similarly named record series on various RRSs had retention periods of Termination or Superseded.

- Contracts / Agreements and Agreements / Contracts: RRSs with these similarly named record series had retention periods varying from Termination + 1, Expiration, and Expiration + 3. Other similarly named record series including contract(s) or agreement(s) in their name had retention periods ranging from Expiration, Expiration (Vital), Expiration + 1, Life of Property, Termination + 1, Termination +7, Life of Company (Vital), Superseded, and Settlement (w/ "H" / historical reference noted).

- Purchase Orders / Requisitions: Finance Purchasing has this record noted with a retention period of Current Year +7. Related or similarly named records on other record schedules have retention periods of Current Year + 1, Current Year + 2, Termination, and Expiration + 3.

- Invoices: of the RRSs observed with this record, retention periods reflected were Current Year or Current Year + 1; DRPA Finance had Invoices with a retention period of C+6 (hand written on RRS provided by OCS).

3) **Key records not noted on RRSs of logical responsible areas:**

- Invoices: this record was only noted on the RRSs of CAO Customer Service and Community Relations, CEO - Deputy CEO, Homeland Security/Emergency Management, Finance Payroll, DRPA Finance, but the Invoice record series was not noted on PATCO Finance, who along with DRPA Finance, retain and process invoices (and the supporting approval documents) through their respective Accounts Payable groups.

- Finance Vouchers: this record was only noted on Engineering’s RRS, the Finance Voucher record series was not noted on the RRSs of DRPA Finance and PATCO Finance who retain and process Finance Vouchers through their respective Accounts Payable groups. (Note: Contract Vouchers, used to facilitate and document invoice approval and associated accounting, was not observed on any RRS provided.)

- Journal Entry Back-Up: this record series was noted on the DRPA Finance RRS as appropriate; however, the retention period was only for Current Year + 3 (total of 4 years) which would appear minimal in terms of retention for a key document of this nature. Most financial records are retained for a minimum period of 7 years. Research of retention periods for journal entries referenced anywhere from 6 – 10 years, including permanent retention.

Review of the RRSs also raised questions associated with interpretation when defining a record / document. There is a need for additional guidance explaining the definition of a record / document, and
allowing the consistent approach and understanding as to what a record category represents and what documentation should be included and retained. At a minimum, clear definition and guidance is needed for:

- contracts / agreements;
- bid documents / quotes;
- bid evaluations;
- associated contract correspondence over the course of the contract;
- miscellaneous correspondence vs. correspondence germane to administering a contract / project or supporting a business decision, etc.; and,
- journal entries and supporting justification (particularly non-recurring, manual journal entries).

**Audit Finding 6:** Review of RRSs identified: inconsistent record naming convention; inconsistent retention periods applied to identically named records and similar records / record series; key records were not noted on RRSs of logical responsible area; and, a need for guidance as to what should be included / retained within a set of records.

**Audit Recommendation 6:** When evaluating / updating the existing RRSs, the Corporate Secretary / General Counsel should develop and communicate guidelines that will promote, at a minimum, a) consistency across the Authority in the naming / definition of records / record classification, b) consistency in associated retention periods, c) assurance that key records are identified in logical responsible areas, and d) guidance as to what should be included within a set of records i.e. contract/procurement documentation, journal entry / justification and approval, etc.).

**Management’s Response 6:** The former Corporate Secretary / General Counsel agreed with the recommendation. While the Corporate Secretary / General Counsel concurred with the issue and recommendation, she could not provide a realistic target date for implementation of corrective actions. The implementation of the corrective actions to address this recommendation will be undertaken as part of the responsibilities of the Records Manager upon their hire. (See Management Response 1.1)

According to existing RRSs, the OCS is currently responsible for retaining Authority related contracts / agreements (Office of Record). There are no controls in place to readily assure that all executed contracts / agreements are on file. Also, there is no guidance as to what contracts / agreements the OCS is accountable for retaining, nor the level of documentation supporting the associated procurement process (i.e. authorized contract/agreement, authorized SS&R, Request for Proposal - RFP, Request for Quotation - RFQ, associated vendor quotations / bids, contract award analysis and award justification, etc.). One area within the Authority should be accountable to retain the complete documentation supporting the Authority’s contracts / agreement procurement process from “cradle to grave”.

15
Currently, contract documentation can be dispersed across various entities within the Authority, including OCS, Contract Administration, Purchasing (DRPA / PATCO), and the responsible area managing compliance of the awarded contract / agreement.

**Audit Finding 7:** There are no controls in place to readily assure that all executed contracts / agreements are on file. Also, there is no guidance as to what contracts / agreements the OCS is accountable for retaining, nor the level of documentation supporting the associated procurement process (i.e. authorized contract/agreement, authorized SS&R, RFP, associated vendor quotations / bids, contract award analysis and award justification, etc.).

**Audit Recommendation 7:** The Corporate Secretary / General Counsel should evaluate the current method of documenting and retaining all procurement related supporting documentation for the life of all Authority contracts / agreements, and establish documentation standards and accountabilities. Once established, the new documentation and retention requirements should be communicated and recorded on the RRSs of the applicable responsible areas. The Authority’s procurement policies and procedures should be revised to reflect the new documentation standards, requirements, and accountabilities. OIG believes that original, approved contracts / agreements (and all other records associated with contract award, administration, and fulfillment) associated with the operation of the Authority should reside within a centralized and controlled area within the Authority; working copies of the contracts / agreements should be provided to the responsible area assigned to administer the contract. Other non-service, non-project, or non-commodity related contracts / agreements can continue to be retained within the OCS or OGC.

**Management’s Response 7:** The former Corporate Secretary / General Counsel agreed with the recommendation in principle, but believed the centralized and controlled filing areas should reside within OCS or OGC. Any changes to current practices will be reviewed and implemented as part of the responsibilities of the new Records Manager upon their hire.

**F. Procurement Process**

Summary Statement and Resolution (SS&R) DRPA- 12-044 provided Board authorization for DRPA staff to negotiate the terms of a contract with Iron Mountain for the provision of off-site storage of DRPA records. The Board action was performed on April 18, 2012, and approved funding not to exceed a total of $200,000 for the next five years. Agreement GN-0008-12 between DRPA / PATCO and Iron Mountain Information Management Inc. was executed and effective May 1, 2012. While the contract indicates it was effective May 1, 2012, OIG noted that the official execution of the contract did not occur until on, or after, August 22, 2012 (approximately 4 months subsequent to the effective date). The approved contract was date stamped by Iron Mountain’s Corporate Counsel on August 22, 2012 representing the date of his review and approval. The new agreement governs five individual accounts with Iron Mountain: PE088 (DRPA Storage), PE089 (PATCO Storage), DRPAV (DRPA Climate Controlled Storage), PE964 (Corporate Communications), and 109672 (Information Systems).
**Contract Pricing / Pricing Schedule:**

The pricing schedule(s) included within the contract documentation provided did not reflect all prices invoiced. According to OIG discussion with an Iron Mountain representative, not everything could be included on the proposal since they (Iron Mountain) were specifically told to stay within the page limit of the RFP form provided by DRPA.

Additional pricing schedules were provided directly to the Administrative Coordinator from Iron Mountain subsequent to the awarding of the contract (via email dated July 30, 2013) reflecting annual price increases for the next 4 years of the contract. These price increases were not reviewed / approved by the Manager, Contract Administration, nor the Corporate Secretary / General Counsel. Iron Mountain’s original proposal (dated September 22, 2011) did include language referencing moderate 3% price increases for years 2 – 5.

**Audit Finding 8:** The pricing schedule(s) included within the contract documentation provided did not reflect all prices invoiced. Additional pricing schedules were provided directly to the Administrative Coordinator from Iron Mountain subsequent to the awarding of the contract; these pricing schedules were not reviewed / approved by the Manager, Contract Administration, nor the Corporate Secretary / General Counsel.

**Audit Recommendation 8:** The Corporate Secretary, working with Contract Administration, should establish procedures that require any addendums (changes) to existing contracts / agreements occurring subsequent to the initial award / approval, to be subject to management review and approval prior to becoming part of the contract terms. Once documented as approved, the new terms should be included and retained with the contract documentation package. Language referencing this requirement should be included within the Authority’s procurement policy / procedure. The expected path of correspondence associated with contract changes should also be communicated to the vendors within the contract language or standard terms and conditions.

**Management’s Response 8:** The former Corporate Secretary / General Counsel agreed with this recommendation. The OCS / OGC will work with Contract Administration management to assure that any addendums (changes) to existing contracts / agreements occurring subsequent to the initial award / approval, to be subject to management review and approval prior to becoming part of the contract terms. This will become effective with the next change to the subject contract.

**Evidence of Competitive Bidding:**

According to correspondence reviewed, and discussions with the Manager, Contract Administration and the Administrative Coordinator, the contracted services were competitively bid. The original documentation supporting the unsuccessful competitor’s (Priority Archives) quote and the associated bid evaluation to support the awarding of the contract could not be located, and was not supplied, by Contract Administration. Contract Administration informed OIG that they currently retain the
unsuccessful bids / proposals for 2 years post contract award (at the time of audit, and request for documentation, 2 years had not passed since the awarding of the contract). On face value alone, this retention period appears too short. Based on review of the RRSs, OIG had not seen the 2 year retention period for unsuccessful bids published, nor authorized.

**Audit Finding 9:** Documentation supporting the unsuccessful competitor’s quote and the associated bid evaluation to support the awarding of the contract could not be located, and was not supplied, by Contract Administration.

**Audit Recommendation 9:** The Chief Financial Officer (CFO) should establish Authority policy and procedural language requiring the retention of documentation supporting the competitive bidding of Authority contracts / agreements (RFP, RFQ, Vendor bids/quotes, Award analysis / justification, etc.). Retention of this type of documentation should be the responsibility of the Authority’s Contract Administration and Purchasing areas. The documentation supporting competitive bidding should be retained with the specific contract / agreement procurement package.

OIG is familiar with retaining procurement / contract related documents for a period of at least 7 years; available Authority Record Retention Schedules (RRS) also reflect 7 year retention:

- **DRPA Legal / Deputy General Counsel Contract Administration**
  Retention period for: Contract Files - Contract Termination / Completion + 7 years;
- **DRPA Finance Purchasing**
  Retention period for: 1) Contract / Agreements / Procurement - Contract expiration + 7 years), 2) Purchase Orders - Current Year + 7 years; and,
- **PATCO Finance Purchasing**
  Retention period for: 1) Agreements/Contracts – Maintenance & Service Contracts - Contract expiration + 7 years, 2) Purchase Orders and Requests for Proposals - Current Year + 7 years.

In addition, OIG requested the retention period requirements in place at the Commonwealth of Pennsylvania and the State of New Jersey for comparison purposes / benchmarking:

- **Commonwealth of Pennsylvania (supplied by Pennsylvania Office of Auditor General):** Completed Acquisition and Awarded Procurement Process Files (… these files include all bids or proposals received for a solicitation whether successful or unsuccessful) – the records are retained for 4 years after the end of the life of the resulting contract or completed acquisition.
- **State of New Jersey (supplied by New Jersey Office of State Comptroller):** Contracts and Amendments File (… includes copies of plans and specifications, bid proposals, progress/performance reports for payment, correspondence, and supporting documentation) – the records are retained for a total period of 7 years after completion of contract (3 years at local agency and additional 4 years at record center).
Based on OIG’s review of the Authority’s submission for the recent FTA Grant Compliance Triennial Review (October/November 2013), and in regard to Authority contract administration and procurement record retention practices, the following was supplied by the Authority: “We retain all procurement records on site for three (3) years after the final payment under a contract. The files are sent to Iron Mountain and retained there for an additional seven (7) years before records can be destroyed.” This statement reflects that all Authority procurement records are retained a minimum of 10 years post contract completion.

OIG also consulted with the Authority’s General Counsel / Corporate Secretary, who has oversight responsibilities of the Authority’s records management function. She was unaware of the current practice of retaining unsuccessful quotes / proposals for only 2 years, and is in support of a consistent retention period for all procurement documents of 7 years, at a minimum.

Management’s Response 9: As mentioned in the OIG findings, upon request “the original documentation supporting unsuccessful competitor’s quote” was unavailable. It is my understanding that this situation of the missing files is extremely unusual. After determining that the support documentation was unavailable within Contract Admin files, Contract Admin did contact the Administrative Coordinator, and OIG was provided with the requested copies of unsuccessful proposals.

After review of recommendations by IG’s office and feedback from General Counsel/Corporate Secretary, I still am uncomfortable with imposition of a seven (7) year retention period without a comprehensive review by Corporate Secretary’s / Records Management office. Until such time that a Records Manager is identified, and the records retention policy is thoroughly reviewed, and consistently applied, I do support an interim halt to destruction of proposals that are close to the “two-year record retention expiration date” presently in place for “unsuccessful bids”.

As indicated in my initial response, Contract Administration does retain the “winning proposal” and contract documentation for a period of seven (7) years. As mentioned earlier, the unsuccessful respondents’ proposals are held for two (2) years. My understanding is that Engineering also has a two year retention period, after termination of the project for unsuccessful bids.

It appears that both PA’s four-year retention policy, and NJ’s seven-year retention policy are both at least 3-4 years old, and my question on these retention timeframes would be whether these timeframes are still considered “best practices” in 2014, and which retention period (four or seven years) is deemed most appropriate for the Authority.

In addition, I do suggest that the review of a retention period give consideration to a “tiered-approach,” or a certain dollar threshold, under which unsuccessful proposals are held for a shorter timeframe. For example, in the past year, the Finance Department initiated a RFP for an
OPEB study, which resulted in a cost of about $8,000 for the study. The study was completed in a three (3) month period. It would seem that retention of all of the proposals, for this small procurement, for a proposed seven (7) period would not be cost-effective, as opposed to a larger or multi-year procurement, for a more sizeable amount, which should be retention for a longer timeframe. A tiered approach might make sense here, reducing potential storage costs, “right to know inquiries”, etc. (Note: The issue of “bid/proposal protest” time periods, probably should be included in any review of retention periods.)

Under this approach, contracts for one year or under would have a different retention period than multi-year contracts. A tiered approach would take into consideration IG and General Counsel’s concerns on having sufficient time to evaluate important, or significant, RFP procurements, including unsuccessful bids/proposals, even after the work on specific contracts had been completed.

In addition to requiring hard copy RFP responses, which are the “official record” determining if a proposer is compliant with the RFP response time deadline, an electronic file should be requested from all proposers, within the RFP procurement document, for our records. It may be appropriate to retain the hardcopy for a minimum period, and use the electronic version, stored on our servers in specifically identified folders, to satisfy an expanded internal retention period. Such an approach would seem to minimize additional costs related to moving from two years to a newly determined retention timeframe.

Presently, the Authority has various projects/initiatives underway which will have a bearing, and perhaps a significant impact, on the corporate records retention discussion, specifically, a new ERP system, electronic contracting system, and General Counsel’s investigation of various records management software systems. It would seem ideal at this point for a comprehensive look at some of these newly emerging issues mentioned above, hopefully by a new Records Manager, to assist the Authority in finalization of records retention for unsuccessful bids/proposals.

The CFO has agreed to implement / has implemented the following:

1. Immediately suspend the destruction of “unsuccessful bid/RFP responses” that are presently scheduled under the 2 year retention period maintained in Contract Administration, and retain all documentation supporting the competitive bidding of Authority contracts / agreements (i.e. RFP, RFQ, Vendor bids/quotes, Award analysis / justification, etc.). The documentation supporting competitive bidding will be retained with the specific contract / agreement procurement package. Retention of this type of documentation will be the responsibility of the Authority’s Contract Administration and Purchasing areas.
2. Working with the Corporate Secretary / General Counsel, and upon the hiring of the new AGC / Records Manager, Finance will draft policy language that will be shared with Authority Chiefs and Directors, for their information and communication to their staff. The language will inform the Authority of the retention changes and new requirements / responsibilities noted above. The policy change will be communicated initially via email, contingent upon the hiring of the AGC / Records Manager and their subsequent review / supplied input, and ultimately reflected within the associated RRSs and Authority policy. This policy change shall remain in effect until any further update and instruction from the Corporate Secretary / General Counsel.

3. Incorporate a requirement in all RFPs that electronic responses be included as part of the full proposal package; this way, if the retention period is moved beyond two years to a longer length of time, DRPA will have the electronic files to minimize storage issues. Incorporation of this requirement in procurement activities managed through Contract Administration has been implemented.

Audit Clause:

OIG did note that the contract with Iron Mountain included an appropriate audit clause.

National Archives and Records Administration (NARA) Compliance Requirement:

In Iron Mountain’s proposal (dated September 2011), they responded to the following DRPA requirements within the associated Request for Proposal (RFP):

“The DRPA requires that the successful bidder certify its commitment to meeting National Archives and Records Administration standards for storage of Federal records (36 CFR 1228 [Subpart K]). Describe your plan to meet these requirements and the time frame within you is committed to meet the requirements.”

Iron Mountain’s response: “While Iron Mountain does have several NARA compliant facilities in the country, the closet to the Delaware River Port Authority would be the facility in Fredericksburg, Virginia. Iron Mountain would be glad to help transfer DRPA’s records to this facility.”

The topic of NARA compliance was previously broached by Authority management. Per the previous General Counsel’s (R. Brown) email dated December 9, 2009, the topic of NARA compliance was raised and he stated:

“I have just spoken with Ellen Zimmerman of Naremco. Ellen confirms that the original RFP for off-site storage of our documents did include a requirement that the site be NARA complaint. That provision was not based on any legal requirement; rather it was an effort to identify an industry accepted standard and at that time the NARA standard was the industry standard.
Ellen asked how this came up and I told her that I was not sure but that I thought Iron Mountain contacted us. I assume that the facility in which our records are stored was NARA complaint originally (if that was in the RFP) but somehow is no longer complaint. If that is the case Ellen thinks that they may have a contractual obligation to move the material at their cost. I suggest that someone look at the contract to see whether it requires Iron Mountain to provide NARA compliant storage.

There are FAR (Federal Acquisition Regulations) requirements relating to storage but they apply to contractors who provide services to the Federal Government. Ellen says that Grant Recipients are not covered by FAR.

At this point I have not been presented with any information indicating that the DRPA is legally required to adhere to NARA Standards (although that may be a very good policy to adhere to). As a result my prior response stands; we need to make a policy decision based on someone’s knowing what the implications of NARA or non NARA storage may be. Ellen also told me:

1- There are now standards developed by the Association of Records Managers and Administrators (ARMA.org) which may be of interest.
2- Ellen told me that the Records Retention RFP process has been suspended and she has been asked to have NAREMCO extend its contract for six months. This may have been in response to my memo but I was not aware of this action. I would like to assemble a task force to resume the effort to obtain a Records Management and Retention policy that will include management and retention of electronic records. “

[Note: Ellen Zimmerman of Naremco was a consultant hired by the Authority when the Authority was implementing its records management program in the late 1990’s.]

The need for NARA compliance, as well as the previous General Counsel’s (R. Brown) response, was presented to the former Corporate Secretary / General Counsel for her opinion. The former Corporate Secretary / General Counsel saw value in the previous General Counsel’s (R. Brown) opinion and arguments. The former Corporate Secretary / General Counsel also believed this compliance requirement required additional research to determine if it is or is not applicable to the Authority’s off-site records storage. In addition, the former Corporate Secretary / General Counsel would hope that the Records Manager candidate will have sufficient knowledge to address this compliance matter.

Audit Finding 10: NARA standards require research as to the applicability of the compliance requirements relating to the Authority’s off-site records storage activity.

Audit Recommendation 10: The Corporate Secretary / General Counsel should investigate the NARA standards and determine if applicable to the off-site storage of Authority records. If deemed applicable, measures should be implemented to assure future compliance.

Management’s Response 10: The former Corporate Secretary / General Counsel indicated that NARA requirements were not applicable to Authority related offsite record storage. The NARA
requirements will be explored further upon the hiring of the new Records Manager. (See Management Response 1.1)

G. Invoice Review

OIG reviewed Iron Mountain invoices associated with Agreement GN-0008-12 covering the period May 2012 through April 2013 (paid October 2012 through May 2013). The 47 invoices reviewed totaled $66,480.72, which included $8,347 associated with a Settlement Agreement for the previous Iron Mountain contract. Funding of $200,000 was authorized (for 5 years) per approved SS&R# DRPA-12-044, dated April 18, 2012 (equating to $40,000 / year funding allocation). The invoices were associated with the various Iron Mountain accounts: PE088 (DRPA Storage), PE089 (PATCO Storage), DRPAV (DRPA Climate Controlled Storage), PE964 (Corporate Communications), and 109672 (Information Systems). The following was noted:

- All invoices were effectively traced and agreed with Banner Accounts Payable Report detail.
- All invoices were charged and traced to Account #1100-10031-7570-51 within the Banner accounting system.
- Contract Voucher forms (facilitating approval and payment of contract invoices) reflected accurate invoice detail and all necessary approvals from: 1) Manager, Contract Administration, 2) Project Manager (Administrative Coordinator), and 3) Project Director (Corporate Secretary / General Counsel).

While the Contract Vouchers / invoices are noted as approved by three individuals, it was determined that a detailed approval process (i.e. comparing service activity / volume reported and the associated contracted billing rate) was not performed. OIG was informed that the invoices were reviewed for reasonableness only – in comparison to previously received invoices. Invoices were not traced back to the contract for compliance or to supporting documents to confirm accurate activity was invoiced.

- OIG was informed that the Administrative Coordinator would forward the invoices associated with PATCO storage to PATCO’s Purchasing agent for preliminary for review / approval. At time of audit there was no documented evidence that this preliminary review occurred. OIG recommended that if this control would continue to occur in the future, that the PATCO approval be physically documented on the Contract Voucher / invoice. The Administrative Coordinator concurred and relayed the recommendation to PATCO. Effective with the next processed PATCO-related invoice, OIG confirmed the PATCO Purchasing agent had implemented the recommendation by initialing the invoice indicating his / PATCO’s approval. Final approval remains with those authorizing the Contract Voucher: the Manager, Contract Administration, Project Manager (Administrative Coordinator), and the Project Director (Corporate Secretary / General Counsel).
OIG has not been able to identify any reference in any policy / procedure regarding an invoice approval process – who is accountable, who needs to approve (what level and responsibility), and what needs to be performed.

**Audit Finding 11:** A detailed invoice approval process (i.e. comparing service activity / volume reported and the associated contracted billing rate) was not performed. The invoices were reviewed for reasonableness only – in comparison to previously received invoices. Invoices were not traced back to the contract for compliance or to supporting documents to confirm accurate activity was invoiced.

**Audit Recommendation 11:** The CFO should establish a clear policy and procedure explaining the responsibilities and requirements associated with approving invoices / cash disbursements. Signatures on contract vouchers, finance vouchers, invoices, etc. should represent the performance of a control responsibility assuring the validity of the payment approved and its compliance with any associated contract / agreement. This is one key responsibility associated with many other responsibilities within the contract management process.

**Management’s Response 11:** The CFO concurs with the finding and recommended course of action. The initial drafted policy / procedure has been shared with OIG for review and comment prior to release to the Authority. OIG has met with the CFO and supplied comments / suggestions to the original draft policy. The CFO will continue to work with OIG to finalize the policy language. An instructional email will be communicated to Authority management, followed by the release of a formal policy / procedure. The new policy language will be included / or cross-referenced within the Authority’s newly created Contracting and Procurement Policy (Series # 300) and related policy #400 Expense Accounts. The new policy / procedure will be retained and easily accessible within the Authority’s intranet site. The CFO has provided a goal of communicating the policy to all Authority employees by January 31, 2015.

**Pricing Issues:**

As noted previously within Section F – Procurement Process, OIG was only presented with the original contract document and rates from the Administrative Coordinator. Through discussion with Iron Mountain’s representative, OIG obtained updated pricing schedules for the next 5 years of the agreement and successfully traced additional billed rates to Iron Mountain’s website.

Pricing changes were supplied directly to the Administrative Coordinator. Contract Administration, nor the Corporate Secretary / General Counsel were not involved with the correspondence, nor aware of the increases.

Audit Recommendation # 8, within Section F, addresses this issue.

**Duplicate Payment:**

Storage services / activity associated with the PATCO account (PE089) for the Month of January 2013 were invoiced by Iron Mountain and paid by the Authority twice. The value of this duplicate payment
for services was $404.36. This occurred at the time when the invoicing of PATCO storage activity was being shifted from their previous Purchase Order (PO# 301132) to the new Agreement (GN-008-12). The services were initially billed as part of PO# 301132 (and represented the last invoice for the Purchase Order), and were subsequently invoiced again as part of the invoicing for the new Agreement GN-008-12 (which represented the first PATCO Storage related invoice for the new Agreement). The duplicate billing and payment was confirmed by Iron Mountain’s representatives.

OIG, working with DRPA and PATCO accounting groups, facilitated the receipt of the refunded duplicate payment from Iron Mountain and confirmed it was properly processed. The Contract Voucher balances, reflecting paid to date activity, were also adjusted by Contract Administration to reflect the refund of the duplicate payment accordingly.

**DRPA / PATCO Accounting Issue:**

DRPA Accounts Payable was not aware, nor informed, that PATCO related storage charges were being applied to DRPA’s account since the inception of the new agreement with Iron Mountain and the subsequent invoicing of PATCO storage activity. Since this was identified in its early stages, PATCO charges incurred by DRPA totaled $3,075. PATCO charges were being incurred and paid by DRPA and were not being charged back to PATCO accounts.

Upon confirmation of the issue by the DRPA and PATCO accounting groups, OIG, with DRPA / PATCO accounting groups, Contract Administration, and the OCS, facilitated the implementation of a process improvement. The existing Contract Voucher form was revised to alert accounting personnel who process Iron Mountain invoices when PATCO related services are involved, and requiring appropriate charging of the identified records storage expenses to PATCO. The appropriate accounting adjustments were journalized during 2013 to accurately reflect the respective storage costs for both the DRPA and PATCO.

**H. Iron Mountain On-site Visits**

As part of this audit, OIG visited Iron Mountain’s storage facilities at both Sharon Hill, PA and Malvern, PA. Iron Mountain’s routine processing and physical / environmental controls were highlighted during the tours at both facilities.

**Sharon Hill, PA Facility:**

Iron Mountain’s routine processing and physical / environmental controls were highlighted during the tour. Controls restricting unauthorized access to the facility and its contents, as well as those governing
the protection of the records in storage (i.e. fire suppression, climate controlled environments, etc.) were emphasized by Iron Mountain’s representatives.

DRPA file storage boxes are stored all over the “Philadelphia area”. All boxes are received at the Sharon Hill storage facility (Iron Mountain’s local “hub”) to be entered into their processing control system (Safekeeper Plus); some boxes stay at the Sharon Hill storage area, while others are shipped to other facilities in the Philadelphia area. The chain of custody controls were demonstrated by the Iron Mountain representatives. Barcoding and handheld scanners are used by Iron Mountain to ensure the accuracy of recordkeeping and provide a chain of custody history. The tour also included Iron Mountain’s Transportation Department, including handling at delivery and pick-up.

Storage charges invoiced by Iron Mountain on monthly basis include all boxes associated with the Authority’s accounts, except those boxes “destroyed” or “permanently withdrawn” by the Authority. Storage space is reserved and charged for boxes that have been requested by the Authority from Iron Mountain storage facilities and which will be returned to storage. Unless the Authority indicates that a storage box has been “permanently withdrawn”, the storage boxes requested to be returned to the Authority will continue to be charged by Iron Mountain as monthly storage.

Destruction of records in storage is scheduled and performed off-site from Iron Mountain’s Sharon Hill, PA facility; a certification of destruction is supplied by Iron Mountain after the documents are destroyed. OIG confirmed with Iron Mountain representatives, while on-site at Iron Mountain’s Sharon Hill facility, that there has been no destruction activity for the time period reviewed (contract inception until August 2013). There were two destruction orders noted on the activity report that were cancelled (#172071285 and #173268674).

**Climate Controlled Storage Area – Sharon Hill, PA Storage Facility (DRPAV Account):**

Currently DRPA records retained at Iron Mountain and associated with the DRPAV Account are stored in a “Climate Controlled” storage area. These records are stored in “The Vault” at Iron Mountain’s Sharon Hill, PA facility. This area was intended for storage of electronic media and related material, including microfilm, microfiche, tapes; sensitive government documents are also stored in the vault. According to Iron Mountain, DRPA required increased liability for documents associated with the DRPAV account; as a result, Iron Mountain required the records be stored with the “climate controlled” vault, as it would add an additional layer of security. The vault provides the additional security of storing documents behind hardened, vault doors; it also provides Halon fire suppression and a climate controlled.

Storing documents in the climate controlled vault costs more than standard storage. The documents held in traditional storage are also secure with various level of physical security. Based on review of the inventory list, Iron Mountain indicated OGC / Legal, Human Resources, and other documents are stored in the vault; it appears that the records stored in the vault may not need the additional protection / security and environment provided within the “climate controlled” vault. If deemed appropriate, Iron Mountain could close out the higher priced DRPAV account, transfer the associated storage boxes to the standard storage area, and apply the lower, standard pricing associated with the Authority’s exiting PE088 account at Iron Mountain. OIG informed the former Corporate Secretary / General Counsel and
OGC management of this storage situation during the course of the audit, allowing them the opportunity to observe the “climate controlled” area during their subsequent on-site visit of the Sharon Hill facility.

**Audit Finding 12:** It appears that the records stored in the vault may not need the additional protection / security and environment provided within the “climate controlled” vault. Savings can be achieved by shifting the contents held within Iron Mountain’s “climate controlled” vault to the traditional, standard storage option currently in use for the majority of the Authority’s records stored off-site.

**Audit Recommendation 12:** The Corporate Secretary / General Counsel should evaluate the continued need to retain the records associated with the DRPAV Account that are held within Iron Mountain’s “climate controlled” vault for transfer to normal, traditional storage at Iron Mountain facilities and taking advantage of a potential cost savings opportunity.

**Management’s Response 12:** The former Corporate Secretary / General Counsel agreed with the recommendation. OGC has visited the Iron Mountain storage facility and concurred that the “climate controlled” storage is not required for the documents currently in storage with that designated area. OCS / OGC has had Iron Mountain move the records previously retained within the climate controlled area to the Authority’s other existing Iron Mountain accounts, and associated physical records were moved to standard storage within Iron Mountain’s facility. The transfer of documents has been completed, eliminating one invoice to process each month, as well as saving the DRPA $ 753.60 / year. Remaining account PE088 have been set to strict access, allowing only those personnel the former Corporate Secretary / General Counsel had designated access.

**Malvern, PA Facility:**

OIG scheduled a tour of Iron Mountain’s Malvern, PA facility which stores the Authority’s Information Services (IS) related system back-up files. At the time of this visit (September 2013), the DRPA had 3,345 Backup tapes in inventory. As part of the tour, the following was highlighted:

- Physical security / environmental controls (to ensure integrity and preservation of back-up media).
- Vaults (Open Media and Closed Container Vaults), and associated storage / transaction activity:
  
  **Open Media:** IS provides the weekly backup tapes in an open media container provided by Iron Mountain. The container is locked by Iron Mountain, the tapes are removed, scanned / logged, and compared to IS distribution list. If any discrepancies are noted, Iron Mountain’s Securebase system will notify Iron Mountain representatives, as well as DRPA contacts, that there is a discrepancy in need of correction. This represents the current process of storing back-up media.
Closed Container: IS places back-up tapes in a closed container, locks the container, and provides the locked container to Iron Mountain for storage. IS maintains the key for the closed containers stored on-site at Iron Mountain’s Malvern facility (this was confirmed with DRPA’s Director, IS). Iron Mountain cannot access the container, and enclosed tapes. This represents the Authority’s initial method of storing back-up media; however, during the course of storing back-up media at Iron Mountain, the DRPA changed over to the previously defined “open media” method of storage.

- “Walk thru” of Iron Mountain’s receiving and delivery process.
- Chain of custody controls and reliance on barcoding.
- Iron Mountain’s Processing Area / Securebase and SecureSync Systems (Securebase is Iron Mountains internal system for controlling processing and inventory, similar to Safekeeper Plus system employed at Iron Mountain’s Sharon Hill facility. SecureSync is Iron Mountain’s web-based customer interactive system (utilized by DRPA Information Systems Department), which provides weekly Distribution Lists detailing the weekly back-up tapes provided to Iron Mountain).
- Loading dock / security.
- Invoice billing activity / explanation of invoiced costs.
- Built-in redundancy for power (PECO Energy is the primary supplier; however, Iron Mountain routinely tests back-up fuel-based power generators on their premises) and telecommunication (ATT T1 lines are the primary source, with cable backup).
- All Iron Mountain processes are detailed within their Corporate Operating procedures (all employees must go through a 6 week orientation program prior to touching a tape).

While on-site at the Malvern facility, the Iron Mountain representative informed OIG that they have not been associated with any Disaster Recovery activity (including drills or testing) per their Securebase system records. In addition, per Iron Mountain’s Securebase system records, no tapes in storage had ever been requested by or returned to the DRPA (... no rotation, no testing, no Disaster Recovery drill, etc.).

Based on discussion with the Iron Mountain representative, and review of system generated reports, it was noted that the Director, IS, a Systems Administrator, and the Administrative Coordinator have “E” level access – granting them full web-based access, rights, and authority to make changes to this account, including requesting media destruction. Any of the three DRPA employees noted can solely add / delete individuals with access, and change the level of access / authority. For example, the System Administrator or the Administrative Coordinator could remove the Director, IS from the Iron Mountain system with their current system authority levels. At the present time, the approval of two “E” level users is required to move forward on destruction requests, as well as Disaster Recovery requests. Iron Mountain has confirmed that according to their system records there have not been any destruction requests from this account. OIG’s review of the contact information for the three DRPA employees indicated the email address for the Administrative Coordinator was entered inaccurately within Iron Mountain’s system; as a result, she would not have been receiving any emailed communication
regarding any issues encountered with this Iron Mountain account / facility. Communication would have still been forwarded to the Director, IS and the System Administrator. In addition, the Corporate Secretary / General Counsel, who is ultimately responsible for the Authority’s Records Management Program did not have authorization to access the system, nor authorize / approve the destruction of any Authority back-up files in storage. When discussed with Iron Mountain management, they suggested Authority management should add another layer of employees on the authorization list (with reduced authority), and routinely review accuracy of the Iron Mountain website’s authorization list.

**Audit Finding 13:** The Corporate Secretary / General Counsel does not have authorization to access Iron Mountain’s web-based system, nor authorize / approve the destruction of any Authority back-up files in storage. The Director, IS, a Systems Administrator, and the Administrative Coordinator have “E” level access to Iron Mountain’s web-based system – granting them full web-based access, rights, and authority to make changes to this account, including requesting media destruction. The email address for the Administrative Coordinator was entered inaccurately within Iron Mountain’s system; as a result, she would not have been receiving any emailed communication regarding any issues encountered with this Iron Mountain account / facility.

**Audit Recommendation 13:** The Corporate Secretary / General Counsel should obtain access to Iron Mountain’s web-based system associated with the Authority’s electronic records / back-up files held in off-site storage. The current employees who have access and levels of authority should be reviewed and revised as deemed appropriate for the associated level of risk / responsibility. Particular attention should be focused on who can add/delete/change an individual and the authority levels within the system. Since the Corporate Secretary / General Counsel is accountable for the Authority’s Record Management Program, she should also have mandatory / final system authority to approve any record destruction request (... which is similar to the document destruction request process for paper / hard-copy records stored off-site at Iron Mountain). If it is determined that the Administrative Coordinator is to remain active on Iron Mountain’s system, her correct contact information should be provided to Iron Mountain for adjustment within their system.

**Management’s Response 13:** The former Corporate Secretary / General Counsel agreed with this recommendation. As a result of OIG communicating the issue to the former Corporate Secretary / General Counsel during the course of the audit, the former Corporate Secretary / General Counsel was added to the Iron Mountain web-based system’s list of the Authority’s authorized employees (effective September 24, 2013). The former Corporate Secretary / General Counsel has “E” level access and privileges. Approval levels / requirements within the Iron Mountain system also were changed requiring Corporate Secretary / General Counsel authorization for record destruction requests.

While at Iron Mountain, their representative conveyed that an area for improvement would include Information Services’ response to Corrective Action Requests (CARs). Corrective Action Requests are automatically emailed from Iron Mountain’s Securebase system to Authority provided contacts when
the contents of the Open Media Transport Case do not match the list of back-up files entered on Iron Mountain’s Securesync.com website by Information Services’ personnel. Iron Mountain was having difficulty in contacting IS in an effort to resolve discrepancies and maintain an accurate inventory. Information Services was having a similar problem. The Director, IS informed OIG that when IS personnel attempt to call Iron Mountain to resolve outstanding issues, they are told that someone from Iron Mountain will return their call, but it does not happen; additional follow-up attempts are also unsuccessful. OIG followed up with Iron Mountain after our on-site visit and was informed that improvement was noted in responding to the CARs. According to Iron Mountain management, IS started to forward distribution files when sending back-up media to Iron Mountain; Iron Mountain management expressed that this is a critical part of the chain of custody process as it ensures the proper verification of media movement between both the Authority and Iron Mountain.

**Audit Finding 14:** An opportunity for improvement associated with ineffective communication was conveyed from both IS and Iron Mountain relating to addressing Corrective Action Requests (CARs). Recent communication with Iron Mountain expressed that improvement was noted.

**Audit Recommendation 14:** The Director, IS, should follow-up with Iron Mountain management to assure effective communication channels are in place to promptly address discrepancies (Corrective Action Requests) and assure and promote inventory accuracy.

**Management’s Response 14:** The Director, IS, will follow-up with Iron Mountain management to discuss ways to further improve the CAR process. IS will initiate this discussion with Iron Mountain by March 31, 2015.

**Iron Mountain’s Web-based Systems / Training:**

The Authority could more effectively utilize the web-based software tools provided by Iron Mountain to manage our records in storage. As part of the services provided by Iron Mountain, the Authority has access to their web-based application. Through discussion with Records Management personnel and Iron Mountain management it was determined that the Authority is not taking advantage of the web-based software which could assist in effectively identifying and managing off-site storage inventory and activity. The opportunities to take advantage of the Iron Mountain web-based system tools are more prevalent relating to the management of hard copy / paper record storage, as opposed to the electronic back-up files retained at the Malvern PA facility. Iron Mountain is available to train Authority employees responsible for interacting with Iron Mountain in the use and capabilities of their web-based system. Iron Mountain is a great resource for questions and guidance for records management and storage.
I. Information Services – Backup and Recovery

The audit scope was not intended to include an audit of disaster recover / system back-up. As a result of the structuring of the Iron Mountain contract and the information exchanged during OIG’s on-site visit at Iron Mountain’s Malvern, PA facility, some testing was performed associated with IS’s Iron Mountain account activity and ensuing related questions.

According to the Director, IS, Authority system back-up files stored off-site at Iron Mountain go back to the mid-1990’s. IS forwards weekly and monthly back-up files, containing transaction history, to be stored off-site at Iron Mountain. In addition, IS retains daily back-up files on-site at One Port Center; these daily back-up tapes are protected for two weeks, at which time they can be overwritten. Back-up files remaining on-site at One Port Center are secured within the Authority’s protected IS Data Center.

The Authority’s most recent Disaster Recovery drill was performed November 2011. A formal report was not prepared or supplied to CFO, executive management, or Board of Commissioners. Weekly back-up files retained on-site within IS were used for this exercise. At the time of OIG’s visit to Iron Mountain’s Malvern, PA facility, back-up files in storage at Iron Mountain have never been tested for disaster recovery purposes according to Iron Mountain management. When conducting future disaster recovery drills, the inclusion of Iron Mountain should be considered in order to evaluate their response time and condition of back-up tapes stored at their Malvern PA facility.

As more records and documents are scanned and saved on Authority servers, the need and cost of storing paper documents off-site should lessen, and the importance of backing-up and recovery of Authority servers, systems, and associated files / data will elevate in its already high level of significance. As the trend toward storing records shifts to electronic media (scanned documents), there is a need to insure the scanning process includes a quality assurance aspect resulting in a clear and legible reproduction and that existing retention period expectations are still observed. In addition, guidance should be established regarding what documents are acceptable in a scanned / reproduced capacity vs. the need to maintain the original paper version on file.

**Audit Finding 15:** The Authority’s Record Management Program procedure does not include guidance regarding when and if scanned copies of documents are acceptable as documents of record.

**Audit Recommendation 15:** The Corporate Secretary / General Counsel should draft and incorporate language within Authority records management policy / procedure that addresses when and if scanned copies of documents are acceptable as documents of record. This guidance should also include compliance requirements to assure the quality of any scanned document represents a clear and legible reproduction of the original. Existing retention period expectations for paper / hard-copy documents should be observed for electronic reproductions, if deemed acceptable by Corporate Secretary / General Counsel.
Management’s Response 15: OGC’s position is that scanned copies of documents are acceptable as documents of record. The applicable policies / procedures pertaining to records management will be revised to incorporate the recommended guidance upon the hiring of the new Records Manager. (See Management Response 1.1)

Audit Finding 16: Based on OIG discussion / correspondence with both IS management and Iron Mountain, the following issues were noted.

- According to the Director, IS, the most recent disaster recovery exercise was undertaken during November 2011. A formal written Disaster Recovery report documenting the Information Service’s disaster recovery process, systems and data tested, and conclusions / opportunities for improvement has not been written by the Authority’s IS Department.
- The results of the most recent Disaster Recovery exercise have not been shared with the Authority’s executive management, or the Board of Commissioners.
- The Authority has a Computer Disaster Recovery policy, Series # 502, issued August 7, 1997 (no revisions); the policy outlines “management” responsibilities associated with Disaster Recovery (including Back-up); accountability is not clearly defined, the back-up policy is not defined (systems/programs/records/data, frequency, retention, etc.), and steps to achieve system recovery are not detailed. The policy does not formally address: 1) definition of the frequency of recovery testing beyond the term “regularly”, 2) internal documentation requirements relating to the testing scope, performance, and results, and 3) formal reporting requirements to executive management and the Board of Commissioners. The Policy does mention that “… data stored on computer media for a prolonged period of time must be tested at least annually to ensure that the information is recoverable.” OIG was not provided with a detailed Disaster Recovery Plan, nor system and data back-up guidance / procedures. The Director, IS confirmed that IS has some procedures, which will get updated / created upon hiring a Business Analyst; technical SOPs were provided detailing the steps to recover systems / data. Best practices suggest an annual testing of recovery procedures. A testing and reporting frequency suitable to the needs and risk appetite of the Authority should be determined, documented, implemented, and followed.
- IS had not interacted with the third party data back-up storage facility (Iron Mountain) in the performance of the most recent disaster recovery testing. IS informed OIG that they have used weekly back-up tapes that reside on-site at One Port Center for recovery purposes. Iron Mountain management did not have any record of requests from the Authority, and IS specifically, for the retrieval of stored electronic records (i.e. back-up tapes).
- The Authority’s off-site storage facility is not visited to physically verify back-up files in storage, assure adequacy of facility, determine compliance with contracted terms, and observe physical security / environmental control practices. According to Iron Mountain, prior to OIG’s visit during September 2013 there was no record of any Authority related site visitation at Iron Mountain subsequent to initiating the storage agreement at the Iron Mountain Malvern PA storage facility. Best practices call for a documented annual visit.
- When drafting an effective and efficient back-up approach and associated off-site file storage, IS should give consideration to shifting from weekly back-up files stored off-site to a
longer back-up period (i.e. monthly, quarterly, annually). Off-site storage costs are invoiced based on the number of physical files in storage. A reduction in the number of files stored at Iron Mountain’s facility will translate to a reduction in related back-up file storage costs.

**Audit Recommendation 16:** The Director, IS, should address and implement the following opportunities for improvement.

a) A formal written Disaster Recovery report should be prepared to document the scope of the exercise and results. This formal report should be submitted / communicated to the Authority’s executive management and Board of Commissioners.

b) The vendor (currently Iron Mountain) providing off-site storage of the Authority’s back-up files should be involved in future Disaster Recovery drills in order for IS to evaluate their response time and condition of back-up tapes stored at their Malvern PA facility.

c) The Authority’s Computer Disaster Recovery policy, Series # 502, should be reviewed and revised to address: 1) assignment of accountability / responsibility, 2) creation and inclusion of formal documentation supporting the Authority’s back-up policy (systems / programs / records / data, frequency, retention, etc.), 3) definition of the frequency of Disaster Recovery testing, 4) internal documentation requirements relating to the testing scope, performance, and results, and 5) formal reporting requirements to executive management and the Board of Commissioners.

d) IS should visit Iron Mountain’s storage facility (Malvern, PA) to assure adequacy of facility, determine compliance with contracted terms, and observe physical security / environmental control practices. Best practices call for a documented annual visit.

**Management’s Response 16:** The Director, IS has reviewed all of the recommendations and offers these responses to each:

a) With the performance of the next Disaster Recovery exercise the Director, IS will create a formal written report documenting the disaster recovery process, systems and data tested, and conclusions / opportunities for improvement. Upon completion of Disaster Recovery testing an Executive Summary of the report and results will be shared with the Authority’s CEO for his communication and inclusion within the CEO report to the Board of Commissioners at the next meeting following the completion of the Disaster Recovery exercise and associated report. The next Disaster Recovery exercise is expected to be performed during the year 2015 (subject to change based on the implementation of the new ERP system and build-out of the Commodore Barry Bridge Disaster Recovery site).

b) It is agreed that Iron Mountain should be included in future disaster recovery drills. It should be noted that there have been many occasions over the past years where tapes have been recalled from Iron Mountain. During those calls we experienced no issues with the response time or the condition of the tapes. In addition, there are no issues with the restoration of the requested files.

With the performance of the next Disaster Recovery exercise IS will include Iron Mountain (external back-up storage facility) in order to evaluate their performance and quality of tapes maintained in storage at their facility. The next Disaster Recovery exercise is expected to be performed during the year 2015 (subject to change based on the implementation of the new ERP system and build-out of the Commodore Barry Bridge Disaster Recovery site).
c) It is agreed that Policy #502 requires revision. As was stated above, it was the intention to have an IS Business Analyst review all policies and procedures and provide all necessary modifications; however, due to budgetary restrictions that hire has been postponed. IS will make every effort to complete this work but cannot commit to a completion date. The following response / corrective actions are provided to address the specifics within Audit Recommendation #16c:

1) **Assignment of accountability / responsibility** – accountability and responsibility to perform Disaster Recovery testing resides with the Director, Information Services.

2) **Creation and inclusion of formal documentation supporting the Authority’s back-up policy (systems / programs / records / data, frequency, retention, etc.)** – this will be addressed upon the revision of Policy #502 and creation / revision of departmental procedures to be performed by IS Business Analyst (upon his/her hire). In an effort to address this recommendation near term, the Director, IS will pursue contracted assistance using other contracted resources in order to commence policy / procedure creation and revision by March 2015 and potentially complete by September 2015.

3) **Definition of the frequency of Disaster Recovery testing** – starting in year 2015, it is IS’s goal to perform a Disaster Recovery exercise on an annual basis.

4) **Internal documentation requirements relating to the testing scope, performance, and results** – the requirements will be defined within the updated policy and procedures and reflected within the written report developed for each Disaster Recovery exercise (also see response to C2 above).

5) **Formal reporting and communication requirements to executive management and the Board of Commissioners** - this requirement will be defined within the updated policy and procedures (see response to C2 above), and reporting will be initiated with the performance of the next Disaster Recovery exercise (anticipated to be performed and completed during year 2015).

d) IS disagrees with this recommendation, and believes, as the guardian of the DRPA records, it should be the responsibility of the Corporate Secretary to make documented annual visits.

**OIG Response:** Based on the Director, IS’s response above, OIG proposed this recommended responsibility to the former Corporate Secretary / General Counsel, who agreed to perform the onsite visit of the offsite record storage facilities on an annual basis, and contingent upon hiring the new AGC (See Management Response 1.1). OIG believes that in order for this visit to be truly effective IS representation / involvement is essential. The Director, IS concurred.
J. Training / Communication

Based on the responses to the internal control questionnaire / survey, communication with those accountable for records management oversight, and noted audit finding, there is an apparent need for formalized records management training and/or published guidance.

The expectations of a properly structured retention schedule, as well as an overarching records management program, should be communicated frequently and thoroughly within the Authority. The importance of information / document management, including information protection, should be routinely communicated / emphasized throughout the Authority. Recognizing records management as a key component of any company’s infrastructure, the Authority should:

- Introduce the Records Management Program to new employees as part of the New Employee Orientation program;
- Develop / revisit policies, procedures, guidelines and make them clearly identifiable and easily accessible via the Authority’s intranet;
- Designate and train “champions” within the Authority’s various Departments to act as local resources in addressing routine records management questions;
- Periodically remind all employees via broadcast emails / newsletters about the importance of records management, key elements of the records management program, and reinforce their responsibilities;
- Create and post materials throughout the Authority reminding employees about the importance of records management and maintaining compliance with records management policy / procedures; and,
- Identify and communicate key contacts with the OCS and OGC / Legal to address any questions pertaining to the Records Management Program.

Training Manual

During the planning phase of this audit, OIG uncovered a detailed, records retention training manual on the DRPA intranet (E.NET); this online manual was last revised August 2003 (content editor Mike DiGiam). This detailed manual is hidden within the intranet and not readily visible to / publicized for Authority employees. The training manual is associated with the Administrative Services Division which is no longer in existence. The training manual needs to be revisited and updated to reflect the current Authority expectations, organization, and roles / responsibilities associated with records management. This resource, once updated, also needs to be communicated, more prominently displayed, and readily available for reference by Authority employees.

Audit Finding 17: When the Authority’s initial Records Management Program was developed and implemented there was evidence of formalized training and guidance. Formal training and readily accessible guidance is no longer apparent.
Audit Recommendation 17: In concert with revisiting the guidance associated with the records management program, the Corporate Secretary / General Counsel should implement a formal training / communication plan to: 1) inform new employees of the records management program and responsibilities, 2) make records management policy, procedures, and guidance more visible and accessible to Authority employees, 3) identify and train local records management “champions” within each responsible area, 4) periodically communicate with Authority staff reinforcing records management compliance (i.e. biennial email), and 5) identify and communicate key contacts within the OCS and OGC to address records management related questions / issues.

Management’s Response 17: The former Corporate Secretary / General Counsel agreed with the recommendation. While the former Corporate Secretary / General Counsel concurred with the issue and recommendation, she could not provide a realistic target date for implementation of corrective actions. The implementation of the corrective actions to address this recommendation will be undertaken as part of the responsibilities of new Records Manager upon their hire. (See Management Response 1.1)

K. Internal Control Questionnaire Summary (See Attachment A)

At the onset of the Audit of the Records Management Program, OIG emailed an internal control questionnaire / survey to the respective Chiefs within the Authority in an effort to obtain feedback regarding understanding of the records management program, policy, and perception of compliance. The Chiefs shared the questionnaire with others within their responsible area(s) for their insight / perspective. A total of 35 areas across the Authority responded.

The entire results of the internal control questionnaire / survey have been included within this report and are referenced as Attachment A. In summary, some of the common response themes that were present suggested:

- perception of program compliance and understanding is high;
- inconsistencies in program understanding exist;
- opportunities for training / communication exist;
- cost of stored documents has not been communicated; and,
- the Records Management Program policy is missing a key aspect addressing Authority emails and other forms of stored electronic data.
## Summary of Responses

<table>
<thead>
<tr>
<th>Internal Control Questionnaire / Survey Questions</th>
<th>“Yes” Responses</th>
<th>“No” Responses</th>
<th>Total Responses</th>
<th>% “Yes” Responses</th>
<th>% “No” Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Are you aware of, and familiar with, DRPA &amp; PATCO Policy #212 Records Management Program?</td>
<td>34</td>
<td>1</td>
<td>35</td>
<td>97%</td>
<td>3%</td>
</tr>
<tr>
<td>2. Is a formal Records Management Program currently in place, operational, and effective within your responsible area(s)?</td>
<td>32</td>
<td>3</td>
<td>35</td>
<td>95%</td>
<td>5%</td>
</tr>
<tr>
<td>3. If not yourself, have records coordinators been appointed within your responsible area(s)?</td>
<td>28</td>
<td>6</td>
<td>34</td>
<td>82%</td>
<td>18%</td>
</tr>
<tr>
<td>4. Do you have a current, formal, and documented records retention schedule for your responsible area(s)?</td>
<td>32</td>
<td>3</td>
<td>35</td>
<td>91%</td>
<td>9%</td>
</tr>
<tr>
<td>5. Does your Records Retention Schedule include:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. All of the records / documents which you handle in the normal execution of your responsibilities?</td>
<td>32</td>
<td>3</td>
<td>35</td>
<td>91%</td>
<td>9%</td>
</tr>
<tr>
<td>b. Vital records?</td>
<td>26</td>
<td>9</td>
<td>35</td>
<td>74%</td>
<td>26%</td>
</tr>
<tr>
<td>c. Retention time periods?</td>
<td>33</td>
<td>2</td>
<td>35</td>
<td>94%</td>
<td>6%</td>
</tr>
<tr>
<td>6. Have the records and retention time periods been approved by unit management?</td>
<td>31</td>
<td>3</td>
<td>34</td>
<td>91%</td>
<td>9%</td>
</tr>
<tr>
<td>7. Are the records and retention periods in compliance with operating needs?</td>
<td>32</td>
<td>3</td>
<td>35</td>
<td>91%</td>
<td>9%</td>
</tr>
<tr>
<td>8. Are the records and retention periods in compliance with statutory and regulatory requirements?</td>
<td>33</td>
<td>1</td>
<td>34</td>
<td>97%</td>
<td>3%</td>
</tr>
<tr>
<td>9. Have your records and retention periods been reviewed and authorized by the Legal Department?</td>
<td>29</td>
<td>5</td>
<td>34</td>
<td>85%</td>
<td>15%</td>
</tr>
<tr>
<td>10. Does your Record Retention Schedule address electronic data maintained on:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. Authority system servers?</td>
<td>16</td>
<td>18</td>
<td>34</td>
<td>47%</td>
<td>53%</td>
</tr>
<tr>
<td>b. Portable computing devices (i.e. Laptops, Tablets, IPads, etc.)?</td>
<td>2</td>
<td>32</td>
<td>34</td>
<td>6%</td>
<td>94%</td>
</tr>
<tr>
<td>c. Portable / external electronic data storage devices (i.e. thumb drives, CDs, DVDs, hard drives, etc.)?</td>
<td>4</td>
<td>30</td>
<td>34</td>
<td>12%</td>
<td>88%</td>
</tr>
<tr>
<td>d. Cellular / Smart phones?</td>
<td>2</td>
<td>32</td>
<td>34</td>
<td>6%</td>
<td>94%</td>
</tr>
<tr>
<td>11. Does your Record Retention Schedule address emails?</td>
<td>6</td>
<td>29</td>
<td>35</td>
<td>17%</td>
<td>83%</td>
</tr>
<tr>
<td>12. Are all of your records / files well organized, labeled, indexed, appropriately identified, and maintained to allow for accurate and prompt retrieval?</td>
<td>35</td>
<td>0</td>
<td>35</td>
<td>100%</td>
<td>0%</td>
</tr>
<tr>
<td>13. Do you retain records / files on site?</td>
<td>34</td>
<td>1</td>
<td>35</td>
<td>97%</td>
<td>3%</td>
</tr>
<tr>
<td>14. Do you retain records / files offline, but within other Authority facilities?</td>
<td>8</td>
<td>27</td>
<td>35</td>
<td>23%</td>
<td>77%</td>
</tr>
<tr>
<td>15. Do you retain records / files offline at an Authority approved vendor / external records storage facility?</td>
<td>19</td>
<td>16</td>
<td>35</td>
<td>54%</td>
<td>46%</td>
</tr>
<tr>
<td>16. Do you have a formal, executed contract with the external storage facility?</td>
<td>25</td>
<td>10</td>
<td>35</td>
<td>71%</td>
<td>29%</td>
</tr>
<tr>
<td>a. Is this contract specifically for your responsible area(s)?</td>
<td>4</td>
<td>28</td>
<td>32</td>
<td>13%</td>
<td>87%</td>
</tr>
<tr>
<td>b. Is this contract an Authority-wide contract, covering the entire Authority?</td>
<td>3</td>
<td>30</td>
<td>33</td>
<td>91%</td>
<td>9%</td>
</tr>
<tr>
<td>17. Are you familiar with the costs associated with external file storage and associated records management activities?</td>
<td>5</td>
<td>30</td>
<td>35</td>
<td>14%</td>
<td>86%</td>
</tr>
<tr>
<td>18. Do you, or your designee, review and approve invoicing associated with external record storage activities?</td>
<td>4</td>
<td>31</td>
<td>35</td>
<td>11%</td>
<td>89%</td>
</tr>
<tr>
<td>19. Do you, or a designee, monitor your responsible area’s external storage costs?</td>
<td>2</td>
<td>33</td>
<td>35</td>
<td>6%</td>
<td>94%</td>
</tr>
<tr>
<td>20. Are you responsible for transferring your on-site records / files to the external storage facility?</td>
<td>26</td>
<td>9</td>
<td>35</td>
<td>74%</td>
<td>26%</td>
</tr>
<tr>
<td>a. If yes, is the transferring of records / files of site subject to the approval of the Corporate Secretary / General Counsel, Legal?</td>
<td>17</td>
<td>15</td>
<td>32</td>
<td>53%</td>
<td>47%</td>
</tr>
<tr>
<td>21. Are you aware of the destruction of Authority records (within the past 10 years)?</td>
<td>15</td>
<td>20</td>
<td>35</td>
<td>43%</td>
<td>57%</td>
</tr>
<tr>
<td>22. Are you aware of the destruction of records / files within your responsible area (within the past 10 years)?</td>
<td>21</td>
<td>13</td>
<td>34</td>
<td>62%</td>
<td>38%</td>
</tr>
<tr>
<td>23. Have you ever approved the destruction of Authority records?</td>
<td>18</td>
<td>17</td>
<td>35</td>
<td>51%</td>
<td>49%</td>
</tr>
<tr>
<td>a. If no, are you aware of any employee(s) currently, or formally, within your responsible area(s) that has approved the destruction of Company records?</td>
<td>10</td>
<td>16</td>
<td>26</td>
<td>38%</td>
<td>62%</td>
</tr>
<tr>
<td>24. Prior to any destruction of records / files were the contents evaluated to assure they were not deemed necessary to the Authority for vital administrative, legal, fiscal, or historical purposes?</td>
<td>24</td>
<td>7</td>
<td>31</td>
<td>77%</td>
<td>23%</td>
</tr>
<tr>
<td>25. Was the destruction of the records / files performed at the instruction of, or with the approval by, the Authority’s Corporate Secretary / General Counsel, Legal?</td>
<td>24</td>
<td>8</td>
<td>32</td>
<td>75%</td>
<td>25%</td>
</tr>
<tr>
<td>26. Do you retain and maintain records associated with the transferring to and retrieval from the external storage facility?</td>
<td>18</td>
<td>17</td>
<td>35</td>
<td>51%</td>
<td>49%</td>
</tr>
<tr>
<td>27. Do you retain and maintain records associated with the documentation authorizing destruction of any Authority records?</td>
<td>13</td>
<td>21</td>
<td>34</td>
<td>38%</td>
<td>62%</td>
</tr>
<tr>
<td>28. Do you retain and maintain records associated with the documentation confirming destruction of any Authority records?</td>
<td>5</td>
<td>30</td>
<td>35</td>
<td>14%</td>
<td>86%</td>
</tr>
<tr>
<td>29. Has your Record Retention Schedule been reviewed during the past year?</td>
<td>1</td>
<td>34</td>
<td>35</td>
<td>3%</td>
<td>97%</td>
</tr>
<tr>
<td>30. Has your Records Retention Schedule been updated / revised during the past year?</td>
<td>0</td>
<td>35</td>
<td>35</td>
<td>0%</td>
<td>100%</td>
</tr>
<tr>
<td>31. Has your responsible area(s) Records Retention Schedule and records management practices been subject to review for compliance by Authority’s Records Management staff or by any other internal / external assessment?</td>
<td>20</td>
<td>14</td>
<td>34</td>
<td>59%</td>
<td>41%</td>
</tr>
<tr>
<td>a. If yes, did this occur within the past 10 years?</td>
<td>18</td>
<td>6</td>
<td>24</td>
<td>75%</td>
<td>25%</td>
</tr>
<tr>
<td>b. If yes, did this occur within the past 5 years?</td>
<td>17</td>
<td>8</td>
<td>25</td>
<td>68%</td>
<td>32%</td>
</tr>
<tr>
<td>c. If yes, did this occur within the past year?</td>
<td>0</td>
<td>28</td>
<td>28</td>
<td>0%</td>
<td>100%</td>
</tr>
<tr>
<td>32. Have you, or your designees, ever reached out to the Legal Department for advice associated with your record keeping activities and associated retention / destruction guidance?</td>
<td>17</td>
<td>18</td>
<td>35</td>
<td>49%</td>
<td>51%</td>
</tr>
<tr>
<td>33. Has your Records Retention Schedule and any other associated guidance / requirements been shared with, and clearly communicated to, your employees?</td>
<td>30</td>
<td>5</td>
<td>35</td>
<td>86%</td>
<td>14%</td>
</tr>
</tbody>
</table>

Total 832 680 1512 55% 45%