UNITED STATES
CONSUMER PRODUCT SAFETY COMMISSION

OFFICE OF INSPECTOR GENERAL

AUDIT OF THE FREEDOM OF INFORMATION ACT PROGRAM

Issued: September 30, 2015

U.S. CONSUMER PRODUCT SAFETY COMMISSION
WASHINGTON, DC 20207

Christopher W. Dentel
Inspector General

Tel: 301 504-7644
Fax: 301 504-7004
Email: cdentel@cpsc.gov

Date: September 30, 2015

TO : Elliot F. Kaye, Chairman
Robert S. Adler, Commissioner
Marietta S. Robinson, Commissioner
Ann Marie Buerkle, Commissioner
Joseph Mohorovic, Commissioner

FROM : Christopher W. Dentel, Inspector General

SUBJECT : Audit of the CPSC's Freedom of Information Act Program

The Office of Inspector General has completed its audit of the CPSC's Freedom of Information Act (FOIA) program. A copy of the report is attached.

Overall, we found that the CPSC has a functioning program, but we identified several internal control weaknesses. In addition, we found that the program did not comply with certain policies and procedures mandated by the FOIA.

Management, the Office of the Secretary (OGCOS) and the Office of General Counsel (OGC), has been briefed regarding the findings and recommendations of this audit and given an opportunity to respond to them. Management generally concurred with the findings and either agreed to implement corrective actions regarding these findings or indicated that corrective action had already been taken. Management's written response can be found in its entirety as an attachment to the report.

If you have any questions about this report or wish to discuss it, please feel free to contact me at 301-504-7644 or cdentel@cpsc.gov.

Christopher W. Dentel
Inspector General

TABLE OF CONTENTS

EXECUTIVE SUMMARY

BACKGROUND

The U.S. Consumer Product and Safety Commission (CPSC) Office of Inspector General (OIG) conducted an audit of the CPSC's compliance with the Freedom of Information Act (FOIA), 5 U.S.C. § 552. The purpose of the audit was to determine whether the CPSC has developed and implemented proper internal controls, policies, and procedures to ensure the program complies with FOIA laws and regulations. The FOIA is a Federal law that provides any person the right to submit a written request for access to records or information maintained by the Federal Government. Within the CPSC, the Office of General Counsel (OGC), Office of the Secretariat (GCOS), administers the FOIA Program. In addition, the CPSC's National Injury Information Clearinghouse (Clearinghouse), under the Office of Epidemiology, has direct responsibility for providing responses to requests for incident reports, specifically In Depth Investigation (IDI) Reports. Under Title 16 of the Code of Federal Regulations (CFR), Part 1015.20, requests for IDI Reports are to follow the same procedures used for requests for information processed under the FOIA.

The OIG conducted this audit in accordance with generally accepted government auditing standards. Our audit covered FOIA requests, including fee assessments, processed during the period between October 1, 2008 and September 30, 2013. This included reviewing applicable documents to understand the operations of the FOIA Program and related internal controls, as well as conducting a review of the FOIAXpress system's general and application controls. Finally, we assessed the CPSC's compliance with identified applicable laws, regulations, and provisions of the FOIA.

RESULTS OF EVALUATION AND FINDINGS

This report covers our audit of the CPSC FOIA Program for Fiscal Years (FY) 2008 through FY 2013. Overall, we found that the CPSC has a functioning program, but we identified several internal control weaknesses. In addition, we found that the program did not comply with certain policies and procedures mandated by the FOIA. In summary, our findings include:

1. **Operational Efficiency Could be Improved**

   The CPSC can improve the FOIA program by strengthening operational internal controls to ensure the completion of requests are both within the statutory deadlines and accurate. Based on our assessment of internal controls, we identified several areas where effective internal controls did not exist and/or implementation was not complete:

   Operational Efficiency …Pg. 6

   - Untimely Update of the CPSC FOIA Directive
     - CPSC directives communicate formal policies and procedures for various programs including the FOIA program. We found the CPSC directive associated with the FOIA Program to be outdated and not in-line with current legislation.

- FOIA Training
  - GCOS has not developed a formal training program to ensure individuals charged with completing FOIA requests are adequately educated on current FOIA legislation and are conscious of the CPSC's policies and procedures regarding the FOIA program.

- Lack of Internal Controls over IDI Requests
  - CPSC's Clearinghouse Management has not developed written procedures to ensure the proper processing of requests for IDI Reports in accordance with the FOIA. Further, Management has not provided guidance or performed supervisory review over work performed by the Clearinghouse Program Analysts.

- Inadequate Recordkeeping
  - Between FY 08 and FY 13, the CPSC reported 13,761 more FOIA requests to the Department of Justice (DOJ) then actually entered into the FOIAXpress system used by the CPSC to track its FOIA requests. GCOS management was unable to provide documentation to support the variance between the number of FOIA requests reported to DOJ and FOIA requests actually entered to FOIAXpress. According to GCOS management, this was due to GCOS not maintaining the records it used to generate its report to DOJ. The discarding of said records is not in accordance with record retention guidelines issued by the National Achieves and Records Administration (NARA).

- FOIA Processing and Fee Assessments
  - Based on our review of a sample of FOIA requests, we determined that GCOS does not have proper internal controls in place to ensure that FOIA requests are fulfilled in accordance with statutory requirements. Specifically, we found that GCOS does not follow their own policies and procedures for handling requests, which has led to the completion of requests outside statutory deadlines, a lack of adequate documentation to support processed requests, and improper fee assessments.

- FOIA Fee Reconciliation
  - The CPSC's Division of Financial Services (FMFS) has the responsibility to record and collect fees associated with FOIA requests. To ensure proper recording of fees, FMFS has a Standard Operating Procedure (SOP) in place to perform a monthly reconciliation over FOIA fees. However, we determined FMFS does not always perform the SOP procedure as written.

2. **Noncompliance with Applicable Laws & Regulations**

Noncompliance with Laws & Regs…Pg. 13

The FOIA requires agencies to make available to the public certain information. The CPSC does not comply with certain provisions in the following areas:

- Electronic Reading Room
  - The FOIA requires agencies to publish records in an "indexed" electronic format for public inspection. The CPSC has created an electronic reading room via the CPSC public website (www.cpsc.gov). However, the information available is not

current; having not been updated since 2012, and not indexed using a systematic method, nor is it assessed to determine frequently requested information. Therefore, the Electronic Reading Room does not meet the requirements of the FOIA.

- Updated Fee Schedule
  - The FOIA legislation establishes guidelines for agencies to develop and publish a fee schedule. While GCOS has developed a fee schedule, published in the CFR, the fee schedule does not include all of the statutorily required criteria.

- Lack of Internal Controls over Statistical Reporting
  - The FOIA requires that, on or before February 1 of each year, Agencies submit a report to the Attorney General summarizing annual FOIA activity. In our review of the FY 2013 Report, we discovered that GCOS had not established appropriate internal controls to ensure the report's completeness and accuracy. The report contained all the required elements, but the discarding of supporting documentation prevented the OIG from verifying the completeness and accuracy of the report's data metrics. In addition, we were unable to verify the accuracy of the report and we also discovered that the CPSC FOIA Specialists are not following internal guidelines on processing requests, which is resulting in the understatement of response times on requests conveyed in the report.

3. **Information Technology General Computer (ITGC) Controls Review**

ITGC Controls Review… Pg. 15

The OIG noted that GCOS management has not trained and/or dedicated resources to implement and maintain system security access controls for FOIAXpress. The security control weaknesses identified could potentially result in the unauthorized viewing and/or altering of critical agency documents. Specifically, the OIG identified the following deficiencies:

- Lack of system-specific user access control policies and procedures;
- GCOS Management does not authorize FOIAXrpess users prior to granting access;
- The "Principle of Least Access" within FOIAXpress is not enforced;
- The FOIAXpress default password ("foia") was not changed until the OIG brought this matter to management's attention;
- Periodic reviews of FOIAXpress user access rights are not performed;
- GCOS did not test the FOIAXpress application and database changes in a non-production environment prior to implementing the changes in production;
- The FOIAXpress Privacy Impact Assessment (PIA) is outdated and lacks sufficient detail regarding the risk to individuals resulting from the collecting, sharing storing, transmitting, use, and disposal of their PII; and,
- Periodic reviews of FOIAXpress audit logs are not performed.

MANAGEMENT'S RESPONSE

Management generally concurred with our findings and recommendations. Management was given an opportunity to formally respond to this report in writing. Management's response is located at Appendix D.

RESULTS AND FINDINGS

1. Operational Efficiency Could Be Improved

The Office of Management and Budget's (OMB) Circular A-123, *Management's Responsibility for Internal Control,* states, "management is responsible for establishing and maintaining internal control to achieve the objectives of effective and efficient operations, reliable financial reporting, and compliance with applicable laws and regulations." The Government Accountability Office's *Standards for Internal Control in the Federal Government*, dated 1999, describes internal controls further, by defining specific internal control activities agencies to should have in place "policies and procedures…[to] ensure management directives are carried out" and that control activities are "effective and efficient in the accomplishing the agency control objectives." Within the CPSC, the GCOS administers the FOIA Program. The GCOS is ultimately responsible for implementing effective internal controls to ensure that FOIA requests are processed in a manner that is complete, accurate, and in compliance with the FOIA. However, based on our assessment of internal controls, we identified several areas in which effective internal controls had not been established and/or the implementation of internal controls was incomplete, as follows:

Untimely Update of the CPSC FOIA Directive

The CPSC communicates policies and procedures for various agency operations by directives made available through the CPSC intranet. We identified CPSC's Directive 0770.1, *Information Resources Management, Freedom of Information Act Requests* as the directive that governs the operations of the CPSC's FOIA Program. CPSC management last performed a review of the directive in July of 2006. The Executive Director signed the underlying directive on June 30, 2003. In our review of the directive, we found inconsistencies between the text of the directive and both the current FOIA internal control structure in place at the CPSC and the requirements of the FOIA, 5 U.S.C § 552. The inconsistencies identified, are as follows:

- *Outdated Organizational Structure* – FOIA requests for IDI Reports are processed the CPSC's Clearinghouse sector. As of the date of our audit, the Clearinghouse falls under the Office of Hazard Identification and Reduction, Directorate of Epidemiology. However, the directive currently states that the Clearinghouse section is aligned under the Division of Information Management, Office of Information and Technology Services.

- *Designation of FOIA Public Liaisons* – 5 U.S.C. § 552 (k)(6) states, "the Chief FOIA Officer of each agency shall, subject to the authority of the head of the agency…designate one or more FOIA Public Liaisons". The directive neither mentions Public Liaisons, nor gives a description to their responsibilities.

- *Fee Schedule* – 5 U.S.C. § 552 (a)(4)(A)(i) advises agencies to develop a fee schedule applicable to the processing of FOIA requests. 16 CFR 1015.9 contains the CPSC fee schedule, but the directive only cites "determining or charging fees," where applicable, and does not address the fee schedule explicitly.

- *FOIA Exemptions* – 5 U.S.C. § 552 (b)(1), lists the nine categories of information that are exempt, i.e. not required to be released in response to a FOIA request. The CPSC has issued an appendix 0770.1(c) to the directive listing and describing the FOIA exemption provisions. However, the appendix only lists six of those exemptions stating, "Exemptions 1, 8, and 9 do not normally relate to CPSC records."

- *Processing Procedures* – The directive 0770.1, section (8), *Processing FOIA Requests*, does not provide a complete explanation of the CPSC's procedures for processing FOIA requests from receipt to final response.

- *Statutory Limits* – The directive 0770.1 does not advise agency employees that 5 U.S.C. § 552 (a)(6)(A)(i) requires a response to FOIA requests within 20 working days and that 5 U.S.C. § 552 (a)(B)(i) extends that response time by 10 working days.

- *Form of Requests* – 16 CFR 1015.3 states, "A request for access to records of the Commission shall be in writing." Section 0770.1 (7)(a) of the directive provides instruction for handling requests for information by telephone or walk-in. This procedure is no longer applicable to the current internal control structure.

We determined that the cause of these discrepancies is GCOS management not allocating sufficient time and resources to ensure the directive associated with the Commission's FOIA program accurately reflects current legislation, government wide policies, and procedures. Consequently, the CPSC is susceptible to noncompliance with FOIA and CPSC employees could be processing FOIA requests incorrectly, which could lead to significant weaknesses in internal control.

We recommend:

1. GCOS management review and revise the CPSC FOIA Program directive and related appendices to include current practices being performed and requirements established by the FOIA. We also recommend reviewing the directive periodically and updating it as needed.

FOIA Training

An effective method to ensure that FOIA requests are completed within the appropriate timeframe and consistent with FOIA regulations is to ensure FOIA Specialists and agency staff receives adequate training. Currently, GCOS management has not established a formal FOIA training program; instead, GCOS provides "on-the-job" training for new FOIA Specialists. Specialists are even encouraged to review the DOJ website, to identify training opportunities of interest. Conversely, in our review of the 2013 Chief FOIA Officer Report to the DOJ, GCOS management asserted, "*While the CPSC did not hold an agency FOIA conference, we did provide training to staff throughout the agency who are responsible for performing file searches for FOIA requests and to the FOIA Paralegal Specialists who process FOIA requests*." However, management was unable to provide documentation supporting the validity of the assertion of training held during the period reported, but we noted agency wide training did occur from April 15, 2014 to April 17, 2014.

By not establishing a formal training program to ensure individuals charged with completing FOIA requests are adequately educated on current FOIA requirements and are aware of the CPSC's policies and procedures in this area, the CPSC is susceptible to being noncompliant with the FOIA.

We recommend:

2. GCOS Management develop and implement an annual training and development program for all agency employees involved with requests associated with the CPSC FOIA Program. The training should include education on the FOIA, the CPSC's FOIA procedural requirements/internal controls, and when and how to properly assess fees for FOIA records.

Lack of Internal Controls over IDI Requests

As previously mentioned, the CPSC's Clearinghouse is responsible for completing FOIA requests for IDI reports. Under 16 CFR 1015.20, requests for IDI reports are required to follow the same procedures used for requests for information processed under the FOIA legislation. However, we identified internal control weaknesses that have contributed to noncompliance with 16 CFR 1015.20 and the FOIA regarding the processing of FOIA IDI requests.

The OIG based its conclusion on interviews conducted with the Clearinghouse Branch Chief and two Program Analysts with duties over FOIA IDIs. From the interviews, the OIG found that the Clearinghouse does not have proper procedures in place to ensure that requests for FOIA IDI reports are complete, timely, and accomplished in compliance with the FOIA legislation. Specifically, there is no SOP or written directive to assist in the completion of FOIA IDI requests. Per discussion with the Clearinghouse Branch Chief, due to a lack of resources and other projects having a higher priority, the development of a SOP has not occurred. In addition, CPSC management (both GCOS and the Clearinghouse) does not provide guidance or supervisory review over the work performed by the Clearinghouse Program Analysts. Further, the Program Analysts have not received formal training on the FOIA or how to respond to a FOIA request properly.

The following exceptions were found:

- Both Program Analysts corroborated that requests for IDI reports are accepted via the internet, telephone, fax, or e-mail. 16 CFR 1015.3 states, "a request for access to records of the Commission shall be in writing…an oral request for records will not be considered a request for records pursuant to the Freedom of Information Act". Therefore, request received through the telephone are an "oral request" and are not valid FOIA requests.

- In regards to the FOIA exemptions, we inquired of the Program Analysts as to whether they considered the applicability of FOIA exemptions prior to releasing IDIs. Both Program Analysts indicated they do not identify FOIA exemptions due to the lack of formal training and instruction. They only make sure the files are free from Personally Identifiable Information (PII). However, one Program Analyst stated that he had knowledge regarding FOIA exemptions due to his conducting his own research through the internet and searching other Federal agencies websites.

- In addition, the Program Analysts do not charge fees for requests for IDI files, and 16 CFR 1015.9 does not provide a fee waiver for IDI requests. Consequently, the disclosure letters to the requesters do not convey itemized review time, file search time, and/or duplication fees.

- According to 16 CFR 1015.5, "the Secretary or delegate of the Secretary shall respond to all written requests for records within twenty (20) working days (excepting Saturdays, Sundays, and legal public holidays)" and under unusual circumstances, "the time for responding to requests for records may be extended by the Secretary at the initial stage or by the General Counsel of the Commission at the appellate stage up to an additional ten (10) working days". However, the Program Analysts received instruction to respond to FOIA requests within a 60 to 90 days' timeframe.

- Further, we found that Clearinghouse management does not have a role in the FOIA process, as there is no management review performed over the work by the Program Analysts to ensure completeness, accuracy, and compliance with the FOIA. Both Program Analysts stated that the completion and review of the requests is solely their responsibility, but neither Program Analyst functions in a supervisory or management capacity.

We recommend:

Although the Clearinghouse is responsible for satisfying FOIA IDI request, the CPSC's GCOS is ultimately responsible for the CPSC's FOIA Program. Specifically, this includes ensuring requests are received and processed in accordance with the FOIA.

3. Therefore, we first recommend that the Program Analysts responsible for completing IDI requests in the Clearinghouse are included in the structured annual FOIA training program. The training should include education on the FOIA, the CPSC's FOIA procedural requirements, and when and how to properly assess fees for FOIA records.

4. Following the completion of the training, we recommend that the Clearinghouse with the assistance of GCOS develop a SOP to ensure that the receipt, processing, and tracking of FOIA requests for IDI files is accomplished in accordance with the FOIA legislation.

Inadequate Recordkeeping

Good recordkeeping practices ensure the maintenance of adequate documentation to control the creation and growth of records, improve efficiency and productivity, and safeguard vital information. To assist agencies in developing appropriate recordkeeping policies, the NARA published the General Records Schedule 14, which covers recordkeeping criteria pertaining to information services performed by Government agencies in their day-to-day affairs regarding relations with the public. This includes records (requests files, appeals files, control files, reports files and administrative files) created in administering the FOIA.

Currently, the GCOS has not developed a method to track all FOIA requests received that adheres to the NARA FOIA retention requirements. Thus, the CPSC does not properly maintain

records to support data and information reported to the DOJ and Congress on the performance of the CPSC's FOIA Program.

We reached the above conclusion through our examination of the FOIA request population from the FOIAXpress system form the period October 1, 2007 to September 30, 2013. The FOIAXpress system reflected the receipt by the CPSC of 5,636 FOIA requests. However, according to www.FOIA.gov (maintained by DOJ), the CPSC reported to the DOJ the receipt of 19,397 requests. In other words, there were13,761 more requests reported to DOJ than reflected in the FOIAXpress system. GCOS management explained the variance by stating that not all FOIA requests are entered into the FOIAXpress system. The requests not logged into the FOIAXpress system are "easy requests" that are handled expeditiously via e-mail and requests completed by the Clearinghouse (IDI Reports). GCOS was unable to provide any documentation to support the number of "easy requests" as any logs or e-mails validating these requests are discarded after the relevant reporting period.

We recommend:

5. GCOS begin entering all FOIA requests received into the FOIAXpress system. In the alternative, GCOS could create a systematic method of tracking FOIA requests and responses that do not require electronic filing.

6. We also recommend GCOS develop a record retention schedule that complies with the guidelines established by the NARA, General Records Schedule 14, on properly retaining FOIA requests.

FOIA Processing and Fee Assessments Needs Improving

Having well-written policies and procedures is essential for creating an internal control system that meets operational needs, effectively manages risks, and ensures compliance with laws and regulations. As previously identified, GCOS lacks a formal set of policies and procedures set out in agency directives and SOPs over the FOIA Program. We identified that GCOS has been developing a SOP for processing FOIA requests, but the SOP remains in draft form and contains inconsistencies with the FOIA. For example, we identified that GCOS requires the completion of simple requests in 60 days or less; a complex request is required to be completed in more than 60 days; and an expedited request requires processing in 10 days. However, 5 USC 552 (a)(6)(A) gives an agency a maximum of 30 days (excluding weekends and legal public holidays) to fulfill a request – 20 days after the receipt of the request, and an additional 10 day if an extension is authorized. Through our assessment of internal controls (discussed below – Table 2), we calculated that on average complex and simple requests took 98 and 51 business days to complete, respectively.

In addition, GCOS has prepared and distributed to CPSC employees a *CPSC FOIA Fee Charge Structure* memorandum. We reviewed this memorandum to ensure the fee structure in place is in accordance with 16 CFR 1015.9. We noted the distributed fee structure instructed employees to waive the entire review costs for "other requesters." Other requesters are defined as consumers, consumer groups, and plaintiff attorneys. This exemption is not indicated in 16 CFR 1015.9,

Fees for Production of Records, thus resulting in the CPSC not capturing the appropriate fees associated with processing FOIA requests. According to FOIA.gov, the CPSC was averaging $8.46 in fees for every processed request in FY 11; in FY 13, that average was reduced to $1.20. See Table 1 below.

Table 1

FY	Processed Requests	Fees Collected	Average Fee Collection
2008	3,837	$5,702	$1.49
2009	3,465	$20,330	$5.87
2010	3,195	$6,628	$2.07
2011	2,560	$21,653	$8.46
2012	2,452	$5,533	$2.26
2013	1,946	$2,343	$1.20
Totals	17,455	$62,189.00	$3.56

Source: www.FOIA.gov

In order to further assess the internal controls over the processing of FOIA requests and assessing of fees, we sampled 45 completed requests and noted the following exceptions:

Table 2

Exceptions	# of Exceptions	OIG Comments
Requests logged more than 7 days after receipt	10	GCOS requirement; SOP states 7 calendar days. However, GCOS management states that this should be 7 business days.
No evidence to support proper notification to manufactures (reversal letter) of final decision	5	None
No evidence to support GCOS Management final review/approval of FOIA Requests	4	None
Request did not meet the statutory processing deadlines	33	23 requests identified as Complex; 10 requests identified as Simple
No date stamp of receipt on request	1	unable to determine receipt date
No itemization of fees assessed	39	Fees were waived without explanation

We recommend:

7. The Chief FOIA Officer takes more initiative in monitoring the timeliness and completeness of completed FOIA requests. This should include:
    a. Tracking FOIA requests upon receipt to ensure they are completed within the statutory limit and receive the appropriate fee assessment;
    b. Performing an annual evaluation, with statistical benchmarks, of the CPSC's administration of the FOIA; and,

c. Develop, document, and finalize policies and procedures over the CPSC's FOIA Program and ensure that they are consistent with the current FOIA legislation.

Proper Completion of the FOIA Reconciliation

The CPSC's FMFS has the responsibility to collect and track fees associated with FOIA requests. FMFS monitors the collection of FOIA requests by preparing and reviewing a monthly reconciliation to highlight the fees assessed and to ensure that all FOIA fees are recorded accurately in the CPSC's financial statements.

FMFS has in place SOP AR.08.v1, *Reporting and Reconciliation, FOIA and Civil Fines/Penalties Validation Report*, which outlines the process for reporting and reviewing the status of CPSC's FOIA collections. In assessing the design and implementation of the FOIA reconciliations, we reviewed the reconciliation performed as of December 31, 2012, along with the associated written standard operation procedures. We concluded the performance of the FOIA reconciliation was not adequate to ensure the completeness and accuracy of the FOIA account balance as of December 31, 2012, based on the following:

- The reconciliation included a line item, "Total O/S FOIA debts per Office of Secretary," but when we requested the FOIA logs from FMFS to perform the reconciliation, we were informed they had not obtained the logs to verify the outstanding balance.

- The process involves interaction with GCOS, whom has the responsibility to "verify" the validation report. Specifically, Step 3 of the SOP requires GCOS to review, verify the accuracy of the validation report, and to communicate any necessary corrections to FMFS. We noted there was no evidence to support that GCOS is actually involved in the FMFS validation process.

- While the SOP is titled to include the FOIA reconciliation procedures, it describes only civil penalty collections (another CPSC collection program) reconciliation procedures, and does not give clear instructions to the FMFS Accountant on how to perform the FOIA reconciliation/validation. However, we agree the process identified in the SOP, in general terms, can be used to verify the FOIA account balance.

FMFS has a SOP on how to reconcile FOIA collection activity; therefore, it is unclear to the OIG why the process is not being performed, as written. While the SOP does not clearly indicate how to perform the reconciliation/validation specifically to FOIA, we have concluded that the FMFS staff is sufficiently well versed in performing reconciliations to ensure their performance of the process would be complete.

This weakness in internal control could possibly contribute to significant misstatements of the reported financial statement amounts, which can lead to significant deficiencies and/or material weaknesses over time. Further, the internal control weakness can contribute to inaccurate reporting of the CPSC's financial information, as GCOS may rely on reported collection data to Congress and other regulatory agencies.

We recommend:

8. That FMFS review & revise SOP# AR.08.v1, Reporting and Reconciliation; FOIA and Civil Fines/Penalties Validation report to include steps for completing the FOIA reconciliation/validation report. The reconciliation/validation process should include a review of the Delphi accounts receivable aging report to the GCOS fee logs, and any variances should be investigated/resolved and documented, accordingly. Further, if the revised SOP still requires that GCOS "verify" the validation report completed by FMFS, FMFS must appropriately train GCOS staff to ensure the complete performance of the reconciliation/validation, so that financial report objectives are met.

2. Noncompliance with Applicable Laws & Regulations

Electronic Reading Room Could be Improved

Subsection (a)(2) of the FOIA provides for what is commonly referred to as "reading room" access. It applies to certain basic agency records that, while not automatically published under subsection (a)(1) of the legislation, must routinely be made "available for public inspection and copying" in agency reading rooms. This public inspection obligation applies to all federal agencies, it governs all records covered by subsection (a)(2) except those "offered for sale," and it extends to the maintenance of "electronic reading rooms" as well.

The OIG performed a review of the CPSC's FOIA electronic reading room and determined that although GCOS has established an electronic format for easy access to agency records opportunities for improvement exist:

- Under the section "Frequently Requested Documents, In-depth Investigation and Incident reports, Reports by Topic" section, GCOS lists only three subject areas: crib bumpers, drywall, and recreational off-highway vehicles. We requested the mechanism management used to determine frequently requested topics, and found no performance of such analysis.

- GCOS does not update the FOIA website in a timely manner. Upon review of the "Search for Investigations and Incident Reports by fiscal year" section, we noted that the most recent reports available were from FY 2012.

- GCOS does not always properly index files. We selected the "Recreational off-Highway Vehicles, Consumer Incident Reports" link, which provided a 320-page document. The document contained multiple Consumer Product Incident Reports from various FYs.

Because of the CPSC's GCOS not allocating sufficient time and resources to properly, manage the CPSC's FOIA "electronic reading room," agency records have not been readily available to the public, decreasing responsiveness, and potentially causing FOIA personnel to expend unnecessary time and resources duplicating work previously accomplished.

We recommend:

9. GCOS develop guidance to determine subjects of frequent requests and timely perform updates to the CPSC's electronic reading room.

Outdated Fee Schedule

As previously observed through our test of internal controls over FOIA processing (see the *FOIA Processing and Fee Assessments Needs Improving* section, above), the CPSC's policies and procedures for the assessment of FOIA request fees do not fully adhere to the current FOIA legislation. Subsection (a)(4) of the FOIA requires agencies to develop fee schedule procedures applicable to the processing of FOIA requests and establish guidelines for determining when fees should be waived or reduced. The CPSC GCOS has developed a fee schedule, which is published to the 16 CFR 1015. However, we determined the fee schedule does not include all of the required elements established by the FOIA regulation. Specifically, the schedule does not address the requirement of not assessing fees, if the agency fails to comply with any time limit; or if no unusual or exceptions circumstances apply to the processing of the request.

The effect of CPSC's GCOS not allocating sufficient time and resources to ensure the CPSC's fee schedule is in line with the current FOIA legislation could result in CPSC employees processing FOIA requests incorrectly.

We recommend:

10. GCOS management review and revise the CPSC published fee schedule and ensure the fee schedule is in line with the current legislation. We also recommend the periodic review and update of this schedule, as needed.

Lack of Internal Controls over Statistical Reporting

The FOIA 5 U.S.C. § 552, requires that on or before February 1 of each year each agency submits to the Attorney General of the United States a report of FOIA activity for the preceding fiscal year. In addition, each agency is required to make the raw statistical data used in its reports available electronically to the public upon request. The statistics reported includes: the number of requests received, the number of requests processed, the number of requests pending as of the end of the reporting year, and the median number of days that those requests were pending. Agencies are also required to specify the resources devoted by them to the processing of their requests, in terms of both dollars and full time staff, and to include information about exemption statuses, which they have relied upon to withhold information.

To evaluate CPSC's compliance with the annual report requirements, we obtained and reviewed the CPSC's FY 2013 annual report to the Attorney General. Our review identified two issues. Both issues identified were caused by GCOS not having proper internal controls in place, which could lead to CPSC's noncompliance the FOIA legislation and inaccurate statistical reporting.

- The report contained all of the required data elements; however, we found no internal controls in place requiring the review and approval of the report before submittal or establishing procedures to verify the accuracy of the report's statistical data elements. We found that GCOS does not perform a second level review before submission to DOJ, as the Chief FOIA Officer has sole responsibility for compiling the raw statistical data and completing the report. Further, the raw statistical data used to compile the report was discarded.

- GCOS relies on the FOIAXpress system to calculate the response time of completed FOIA requests. Specifically GCOS uses the "processed days" field, which determines the number of business days needed to process a request from receipt to close. We reviewed the date calculation with the GCOS Technical Specialist and determined that the timing of a FOIA requests starts with the "received date" and ends with the "closed date" field. This methodology would yield an accurate computation of response times. However, we also noted that the FOIA Specialists are populating the "received date" field with the date the FOIA request is uploaded into the FOIAXpress system and not the actual receipt date. This was determined by comparing the time and date stamp indicated on the request to the "received date" in FOIA express.

We recommend:

11. GCOS develop standard operating procedures to compile the annual report to the DOJ. These procedures should include a supervisory review to ensure that report's accuracy.

12. We also recommend that GCOS develop a records retention schedule to facilitate the proper retention of FOIA requests documentation. Included in that schedule should be guidance on properly maintaining the statistical data used to compile the annual FOIA report to the DOJ.

13. In addition, , we recommend GCOS management begin reviewing the data fields to ensure requests are properly entered and processed in FOIAXpress.

3. ITGC Controls Review

GCOS implemented the FOIAXpress system in 2008 to assist in tracking, monitoring, and maintaining FOIA requests and related documentation. As such, the OIG found it appropriate to perform an ITGC controls evaluation as part of the audit to assess the completeness, accuracy, and integrity of the information maintained in FOIAXpress, in support of our audit objective. In performing the evaluation, the OIG used the methodology provided in GAO's Federal Information System Controls Audit Manual (FISCAM), consistent with GAGAS. The FISCAM provides general and business application control categories, which were used to evaluate and assess the CPSC's FOIA IT environment. The ITGC controls results and findings reported below, are application level general control weaknesses specific to the FOIAXpress. However, our audit also identified IT enterprise-level security control weaknesses that affect the FOIA IT environment in the following areas: Configuration Management, Risk Management, Identity and Access Management, Remote Access Management, and Contingency Planning. These findings have already been reported in the CPSC's OIG FY 14 Federal Information System Management Act (FISMA) Compliance Report.

A Lack of System-Specific User Access Control Policies & Procedures for FOIAXpress

Per the National Institute of Standards and Technology (NIST), *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53 Revision 4 (hereinafter referred as "NIST guidance"), *Access Control (AC) – 1, Access Control Policy and Procedures*, the organization should develop, disseminate, and review/update a formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Management should also develop, disseminate, and review/update formal, documented procedures to facilitate the implementation of the access control policy and associated access controls. The OIG conducted an interview with the GCOS Tech Info Specialist, whom serves as the FOIAXpress Administrator, to gain an understanding of the access control process. As a result of this interview, the OIG noted that management has not trained and/or dedicated resources to developing and implementing system specific access control policies and attendant procedures for the FOIAXpress system. Without sufficiently documented policies and procedures outlining the agency responsibilities for information system access, resources assigned to complete these tasks may not understand their responsibilities resulting in potential security weaknesses.

We recommend:

14. Management should draft, approve, implement, and disseminate NIST compliant Access Control policies and procedures for all agency systems including FOIAXpress. Management should pay particular attention to the following topics addressed in the Access Control section of the NIST SP 800-53 guidance when documenting a policy governing and defining metrics for:
    - user authorization;
    - the implementation of role-based security;
    - the implementation of the Principle of Least Privilege;
    - user separation protocol;
    - password metrics (based on a formal E-Authentication analysis);
    - common account control; and,
    - audit log monitoring.

Granting Access to FOIAXpress

The FISCAM states that a manager and the application administrator must authorize the user's level of access before the user obtains a user account and password for the application. This requirement is reiterated in NIST guidance, as control *AC – 2, Account Management*. However, management does not have a formal process in place to ensure that individuals requesting access to FOIAXpress are authorized access prior to granting them access; due to management's inability to train and/or dedicate resources to implementing and maintaining system security access controls. Per the FOIAXpress System Administrator, and corroborated by our testing, when an access request is made, the FOIAXpress System Administrator grants the requestor access without consistently receiving a formal authorization from the requestor's supervisor or

from the system owner. This results in the possibility of critical agency documents being viewed and/or altered by users without a business need to do so, thus increasing the risk of compromising the integrity and confidentiality of these documents. If the confidentiality and/or integrity of these documents is compromised, there is a serious reputational risk to the agency and a serious potential risk to the individual or business to which the documents pertain.

We recommend:

15. Management should implement a formal process to authorize users prior to granting access to FOIAXpress. This authorization should also include the level of access the user be permitted, and the level of access permitted should be based on the minimum level of access required for the user's intended usage.

The Principle of Least Access Use within FOIAXpress

The FISCAM states that management should segregate application user access to conflicting transactions and activities, monitor segregation, and that access should be limited to individuals with a valid business purpose (least privilege). NIST guidance reiterates these requirements, as controls *AC – 2, Account Management* and *AC – 6, Least Privilege*. However, management does not limit access rights to FOIAXpress to the minimum required for a user's business needs. Again, this is due to management having not trained and/or dedicated resources to implementing and maintaining system specific access controls. As a result, the viewing or altering of critical agency documents by users who do not have a business need to do so may occur, thus increasing the risk of compromising the integrity and confidentiality of these documents.

Specifically, we found that users have access to certain permissions, when those permissions should be limited to GCOS Management (the GCOS Director and Supervisory Government Information Specialist) and/or the FOIAXpress System administrator, as follows:

- All FOIAXpress users currently have rights to the "File Cabinet Drawer Privileges" (permission to work with the file cabinet drawers) and the "File Cabinet Drawer" (permission to create, edit, delete file drawers). However, the only users with a business need for these access privileges are GCOS Management and the FOIAXpress System Administrator.

- All users designated to the OS and FOI user groups have privileges to the "System Config," "System Privileges," and "User Mgt" permissions. However, the only users with a business need for this access is the Supervisory Government Information Specialist and the FOIAXpress System Administrator, serving as the designated backup.

In addition, we found that GCOS management had established an excessive number (10) of FOIAXpress administrators, and granted users administrative access, whom do not require this level of access to complete their job function. Further, GCOS Management has not assigned access rights to the FOIA document libraries based on business needs. However, management is in the process of defining which users have mission needs that require access to the specific FOIA document libraries, and has begun assigning rights accordingly.

We recommend:

16. Management should assign privileges within FOIAXpress and the document repository based on the Principle of Least Access.

17. Management should limit the number of users with administrative access to FOIAXpress to one primary administrator and one or two backups.

18. Management should require administrators to utilize a non-administrative user account to perform tasks that do not necessitate the use an administrator account.

19. Management should develop, formally approve, and periodically review a segregation of duties matrix for FOIAXpress and the FOIA document repository.

20. Management should identify all users with rights that permit a conflict of interest or the overriding of application security controls (i.e. users with administrative privileges, users with system configuration permissions, etc.).

21. Management should periodically review the audit logs of user accounts, which allow sufficient access to permit conflicting duties or the overriding of application security controls (such as accounts with administrator privileges).

FOIAXpress Default Password

During the audit, the OIG was able to log in to FOIAXpress using the default username and password, as the default password had not changed since the implementation of FOIAXpress in 2008. The default password, "FOIA," was widely known and easily discoverable, thus representing a significant risk to unauthorized access to FOIAXpress and the data housed within the system. As conveyed in the FISCAM, management should change vendor supplied default passwords during installation. This requirement is also echoed in control *Identification and Authentication (IA) – 5, Authenticator Management*, per NIST guidance. We found that GCOS management was unaware of the security risks associated with not changing the FOIAXpress default password. However, GCOS management remediated the issue immediately upon notification by the OIG.

We recommend:

22. Management should only provide the new password to the system administrator and one backup.

23. Management should formally change the password for FOIAXpress's built-in administrator account every 90 days.

Periodic FOIAXpress User Access Reviews

The FISCAM states that system owners should periodically review access to ensure continued appropriateness. This requirement is reiterated in the *AC – 2, Account Management* control described in NIST guidance. However, the OIG noted that GCOS does not perform periodic reviews of FOIAXpress user access to ensure that access rights remain appropriate; GCOS was unable to provide evidence that such reviews had occurred. As previously mentioned, as with other control weaknesses, management has not trained and/or dedicated resources to implementing and maintaining system specific access controls. As such, the viewing or altering of critical agency documents may occur by users without a business need to do so, thus increasing the risk of compromising the integrity and confidentiality of these documents.

We recommend:

24. Management should perform periodic reviews of FOIAXpress user access to ensure that access rights remain appropriate and retain documentation of the reviews for future follow-up.

FOIAXpress Application and Database Changes in a Non-Production Environment Prior to Implementation

The FISCAM states that management should effectively separate production (i.e. operational) systems from non-production systems, such as testing and development. This requirement is reiterated in the *Configuration Management (CM) – 2, Configuration Change Control*, described in NIST guidance. Testing of operational systems, such as FOIAXpress, should take place in a separate test environment. A separate test environment means an environment that is physically or logically isolated and distinct from the operational environment. If the separation is insufficient, management cannot ensure that activities in the test environment do not affect activities in the operational environment, and information in the operational environment may be transmitted inadvertently to the test environment. However, GCOS was unable to provide evidence to demonstrate that testing of the FOIAXpress application upgrades and database migration occurred in a non-production environment prior to implementation in a production environment. The factor causing this control weakness is that management has not trained and/or dedicated resources to implementing system specific configuration management controls. As a result, management did not create a separate testing environment to assess database changes prior to implementing these changes on the operational system.

We recommend:

25. Management should create a separate test environment for the FOIAXpress database.

26. Management should test all future changes in the non-production environments prior to implementing a change in production.

The FOIAXpress PIA is Outdated and Insufficient

The FISCAM, OMB Memorandum 03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, and NIST guidance, require management to document and implement a privacy risk management process. The required process provides an assessment of the privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of their PII.

The CPSC did perform a PIA for FOIAXpress, but it did not include sufficient detail to allow the reader to gain an understanding of the risk associated with the confidentiality of data residing on the application and its supporting systems. For example, the scope of the PIA does not include the data housed in the FOIA document repository even though this information is accessible through the FOIAXpress application. In addition, management has not updated the FOIAXpress PIA since its implementation in 2008, even though management has implemented significant changes to the application and the underlying infrastructure housing the application's confidential data. This failure to update was caused by management not dedicating sufficient resources to developing and maintaining agency PIAs. If management does not provide sufficient detail in the PIA, the users of this information (e.g., the Public), will not be provided an accurate depiction of how the CPSC is protecting its confidential data.

We recommend:

27. Management should expand the scope of the PIA to include the FOIA document repository. Also, management should update the FOIAXpress PIA to include:
    - The new name of the System Owner;
    - The System Of Record Notice number associated with the FOIAXpress application;
    - The administrative and technical controls management has implemented to ensure that the confidential information within FOIAXpress is adequately protected;
    - The list of users who have access to the system (this list should include the Office of Hazard Identification and Reduction); and,
    - Management should update the FOIAXpress PIA each time a significant system change occurs. This can occur as part of the new Security Impact Assessment.

Periodic Reviews of FOIAXpress Audit Logs

GCOS Management does not review FOIAXpress audit logs on a periodic basis to detect inappropriate or unusual activity. Per inquiry of the FOIAXpress Administrator, certain actions performed by FOIAXpress users are logged within the system. However, the Administrator was unaware that the logged actions are actually retrievable in a report form (audit logs). There is also no documented policy to support the requirement to review FOIAXpress audit logs. The FISCAM states that management should implement adequate audit and monitoring capability. This includes monitoring the use of sensitive/privileged accounts, and the implementation of detective controls to identify and react to specific system or user activity. This requirement is reiterated in the *Audit and Accountability (AU) – 6, Audit Review, Analysis, and Reporting* control, described in NIST guidance. Without such controls, security events may go unidentified and un-remediated, which also limits management ability to minimize the potential damage of the undetected security events.

We recommend:

28. Management should develop a policy or procedure that defines the FOIAXpress audit logs it plans to monitor to identify inappropriate or unauthorized activity. Management should develop this policy in accordance with NIST requirements. Audit logs that should be considered for review include logs that may identify inappropriate or unauthorized usage.

29. Management should delegate the task of periodically reviewing the audit logs to someone without administrative access to the FOIAXpress system and with no operational responsibilities within the GCOS. This will prevent the conflict of interest that naturally arises from an audit log reviewer reviewing his or her own work.

30. The individual(s) responsible for monitoring these logs should formally alert management in the event of inappropriate or unusual activity.

APPENDIX A: BACKGROUND

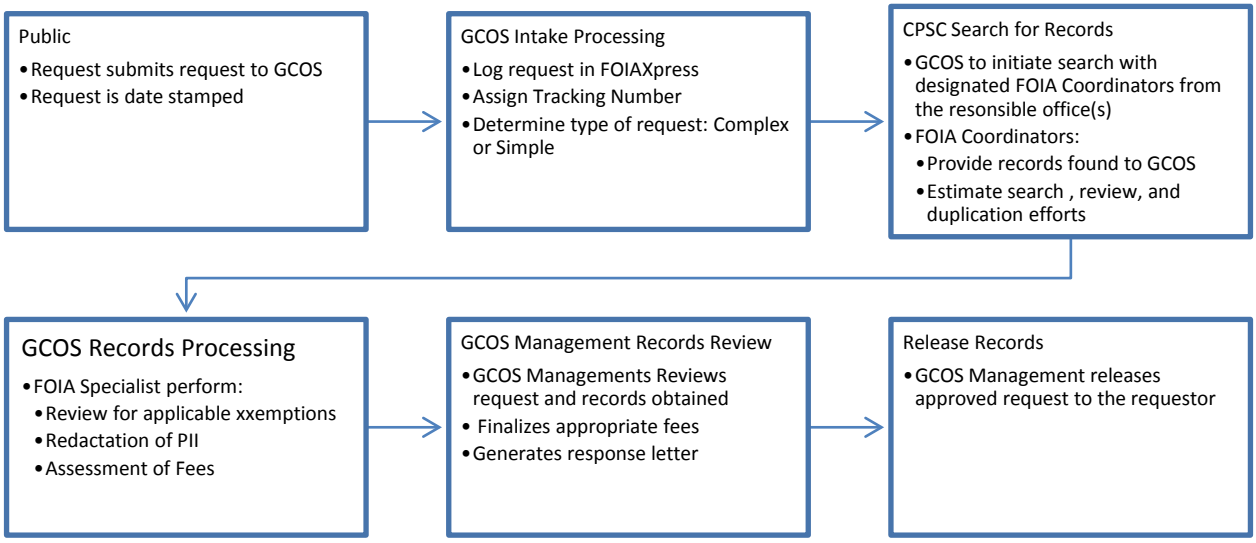
The Freedom of Information Act, enacted in 1966, is codified in Title 5 of the United States Code, Section 552. The FOIA generally provides that any person have a right of access to agency records, with certain exceptions. Agency records that are not available to the public through "reading rooms," are available in response to FOIA requests. All U.S. Government agencies are required to disclose their records or portions of the records, upon receiving a written request. Nine exemptions exist to protect certain information from disclosure under the FOIA (see below). The FOIA was amended in 2007 to narrow the scope of FOIA exemptions and the ability of agencies to withhold information. Each amendment expands the scope of information that is available to the public by the FOIA. Changes implemented demonstrate how Congress and recent Presidential Administrations have been progressively modifying the FOIA to facilitate public access to agency records.

The FOIA's nine exemptions generally cover the following information:

1. Classified national defense and foreign relations information;
2. Internal agency personnel rules and practices;
3. Material prohibited from disclosure by another law;
4. Trade secrets and other confidential business information;
5. Certain inter-agency or intra-agency communications;
6. Personnel, medical, and other files involving personal privacy;
7. Certain records compiled for law enforcement purposes;
8. Matters relating to the supervision of financial institutions; and,
9. Geological information on oil wells

Within the CPSC, the administration, and management of the FOIA Program is the responsibility the CPSC's GCOS. GCOS uses the FOIAXpress IT application to assist in the tracking, monitoring, and maintaining FOIA request documentation.

The following chart summarizes the CPSC's FOIA request process:
Chart 1: FOIA Process Flowchart



APPENDIX B: OBJECTIVES, SCOPE & METHODOLOGY

OBJECTIVES

The purpose of our audit was to determine whether the CPSC had developed proper internal controls, policies, and procedures to comply with the FOIA laws and regulations.

SCOPE

This audit covers FOIA requests processed from October 1, 2008 to September 30, 2013. During this period, the CPSC report to DOJ the processing of 17,455 requests, resulting in the collection of $62,189 in fees and incurred total costs of $8,903,657. All CPSC employees located at the headquarters and field locations throughout the United States were included in the scope of the evaluation. Our fieldwork took place from October 2014 through April 2015.

METHODOLOGY

We conducted this audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

To accomplish our audit objectives, we obtained an understanding of the CPSC's administration of the FOIA program to include the design, implementation, and operating effectiveness of internal controls, compliance with the CPSC governing policies and procedures, and compliance with applicable Federal laws, regulations, and provisions. To obtain this understanding, we conducted interviews with key GCOS personnel, inspected relevant supporting documentation, and examined data from the FOIAXpress system.

Based on the information gathered, we identified specific risks and opportunities for fraudulent, improper, and/or abusive activity related to the program. We also determined what key internal control activities were in place to prevent or detect such occurrences. Additionally, we performed a preliminary assessment of whether the internal controls were likely to be effective and identified any internal control design inefficiencies based on the CPSC's FOIA Program process. From our preliminary assessment, we designed audit procedures (tests of controls) to assess the internal controls' operating effectiveness, to review specific attributes of the program, and to determine compliance with the identified laws, regulations, and provisions governing the FOIA operations.

To perform our procedures at the transactional level, we obtained a population of requests from the FOIAXpress system. To assess the reliability of FOIAXpress's transactional data, we: (1) reviewed related documentation; (2) interviewed CPSC officials knowledgeable about the data; and, (3) verified the completeness of the population by comparing source documents to the requests. We found that one of the data elements, "Received date," may not be reliable, as it is entered in the system inaccurately by GCOS personnel. We identified that this element is used to generate the annual statistical report to congress on FOIA activity, which is the vehicle the CPSC uses to report its FOIA Program's operational efficiency and effectiveness. We issued a

finding to management regarding this issue. See the *Lack of Internal Controls over Statistical Reporting* section of this report for more detail. Based on this assessment, we determine that this particular data element is not sufficiently reliable for the purposes of this report. All other data elements assessed, were deemed sufficiently reliable.

The FOIAXpress FOIA request population from the period of October 1, 2008 through September 30, 2013 included a universe of 5,636 requests. Using the IDEA database, we randomly sampled 45 requests for testing of internal control effectiveness and compliance with the FOIA legislation.

For the ITGC controls evaluation, we assessed the completeness, accuracy and integrity of the information maintained in the CPSC FOIAXpress systems using the FISCAM, dated February, 2009; as well as, agency policies, OMB memorandums, and NIST guidance. As part of this assessment, we interviewed agency personnel, reviewed documentation, and re-performed system specific controls.

Note: The OIG reported enterprise-level security control weaknesses that affect the FOIA systems in the following areas: Configuration Management, Risk Management, Identity and Access Management, Remote Access Management, and Contingency Planning as part of the FY 2014 FISMA Compliance Report. Please see the FY FISMA 2014 Report for these findings at the CPSC OIG Public Website.

APPENDIX C: ACRONYMS & ABBREVIATIONS

Access Control	AC
Audit and Accountability	AU
Code of Federal Regulation	CFR
Configuration Management	CM
Department of Justice	DOJ
Division of Financial Services	FMFS
Federal Information Security Management Act	FISMA
Federal Information System Controls Audit Manual	FISCAM
Fiscal Years	FY
Freedom of Information Act	FOIA
Identification and Authentication	IA
In Depth Investigation	IDI
National Achieves and Records Administration	NARA
National Injury Information Clearinghouse	Clearinghouse
National Institute of Standards and Technology	NIST
Office of General Counsel	OGC
Office of Inspector General	OIG
Office of Management and Budget	OMB
Office of the Secretariat	GCOS
Personal Identifiable Information	PII
Privacy Impact Assessment	PIA
Standard Operating Procedure	SOP
U.S. Consumer Product and Safety Commission	CPSC

APPENDIX D: MANAGEMENT RESPONSE

U.S. Consumer Product Safety Commission Memorandum

TO: Leeann Murphy, Deputy Inspector General (Audit)
Office of the Inspector General (OIG)

THROUGH: Stephanie Tsacoumis, General Counsel
Office of the General Counsel (OGC)

FROM: Alberta E. Mills
The Secretariat - Office of the Secretary
Office of the General Counsel (GCOS)

DATE : September 29, 2015

SUBJECT: The OIG's Final Set of Audit Findings (FOIAXpress) for the FOIA Audit

GCOS has reviewed the audit findings for the FOIAXpress application in relation to the FOIA Audit and we have begun implementing some of the recommendations suggested in the findings. GCOS will continue to make the necessary changes to address all of the audit findings.

Finding 1 – Management did not include sufficient detail in the FOIAXpress Privacy Impact Assessment (PIA) and the PIA is outdated

The OIG audit found that "management did not include sufficient detail in the FOIAXpress PIA to allow the reader to gain an understanding of the privacy risk associated with how the information residing on the application and supporting systems is secured." The audit recommendation states that "the scope of the PIA should be expanded to include the FOIA document repository." The recommendation further states that "management should update the FOIAXpress PIA to include:

- The new name of the System Owner
- The System Of Record Notice number associated with the FOIAXpress application
- The administrative and technical controls management has implemented to ensure that the confidential information within FOIAXpress is adequately protected
- The list of users who have access to the system should be updated to include the Office of Hazard Identification and Reduction
- Management should update the FOIAXpress PIA each time a significant system change occurs."

Response:

We concur with this audit finding. The FOIAXpress system administrator is currently working on the update for the FOIAXpress PIA and will complete this task in the near future.

Finding 2 – Management does not authorize users prior to granting access to FOIAXpress

The OIG audit found that "management does not have a formal process in place to ensure that individuals requesting access to FOIAXpress are authorized to access to FOIAXpress prior to granting them access to FOIAXpress. The audit recommendation states: "Management should implement a formal process to authorize users prior to granting access to FOIAXpress. This authorization should include should include the level of access the user be permitted and the level of access permitted should be based on the minimum level of access required for the user's intended usage."

Response:

We concur with this audit finding and as recommended by the auditor, GCOS will implement a formal process in which management approves authorization prior to granting access to FOIAXpress users.

Finding 3 – The Principle of Least Access is not enforced within the FOIA systems

The OIG audit found that "management does not limit access rights to FOIA systems to the minimum required for a user's business needs.... all users have access to certain permissions, when those permissions should be limited to GCOS management.... and FOIAXpress system administrator." The audit recommendation states in part "Management should assign privileges within FOIAXpress and the document repository based on the Principle of Least Access."

Response:

We concur with this finding and the FOIAXpress system administrator has already taken action to address this finding. The FOIAXpress system administrator will limit user's or a group's access according to their specific roles.

Finding 4 – Management does not perform periodic FOIAXpress user access reviews

The OIG audit found that "GCOS does not perform periodic reviews of FOIAXpress user access to ensure that access rights remain appropriate, as GCOS was unable to provide support of reviews when requested. The audit recommendation states: "Management should perform periodic reviews of FOIAXpress user access to ensure that access rights remain appropriate. Management should retain documentation of the reviews for future follow-up."

Response:

We concur with this audit finding and have begun to implement the recommendations suggested in the audit.

Finding 5 – Management has not changed FOIAXpress default password

The OIG audit found that "management has not changed the FOIAXpress default password since the 2008 implementation. The OIG was able to log into the FOIAXpress application using the default username and password. However, management remediated the weakness immediately upon notification by the OIG." The audit recommendation states: "Management should change the FOIAXpress built-in administrator account's default password. Management should only provide the new password to the system administrator and one backup. Management should formally change the password for FOIAXpress' built in administrator account every 90 days.

Response:

We concur with this finding and took corrective action as stated in the audit findings. GCOS has implemented a system to change the password for FOIAXpress every 90 days as recommended by the audit.

Finding 6 – Management does not perform periodic review of FOIAXpress audit logs.

The OIG audit found that "Management does not review FOIAXpress audit logs on a periodic basis to detect inappropriate or unusual activity." The audit recommendation states in part: "Management should develop a policy or procedure that defines the FOIAXpress audit logs it plants to monitor and identify inappropriate or unauthorized activity. Management should develop this policy in accordance with NIST requirements."

Response:

We concur with this finding and have already taken steps to address this recommendation.

Finding 7 – Management did not test the FOIAXpress application and database changes in anon-production environment prior to implementing the changes on the operations system

The OIG audit found that "GCOS was unable to provide evidence to support testing of the FOIAXpress application upgrades and database migration in a non-production environment prior to implementing in a production environment." The audit recommendation states: "Management should create a separate test environment for the FOIAXpress database. Management should test all future changes in the non-production environments prior to implementing a change in production."

Response:

Management agrees to create a separate test environment for the FOIAXpress database, and to test all future changes in the non-production environments before implementing any change in production.

Please note that the initial roll out of FOIAXpress was tested in a non-production environment for several months prior to implementation in 2008. Also, the first major upgrade and system modification in 2014 of FOIAXpress was tested in a non-production environment as well prior to implementation. The OIG audit finding is correct in that GCOS did not test two software upgrades in a non-production environment prior to installation. We will make certain that all upgrades will be tested in a non-production environment prior to implementation.

Finding 8 – A lack of system-specific user access control policies ad procedures for FOIAXpress

The OIG audit found that "management has not developed and implemented system specific access control policies and attendant procedures for the FOIAXpress system." The audit recommendation states: "Management should draft, approve, implement and disseminate NIST compliance Access Control policies and procedures for all agency systems including FOIAXpress. Management should pay particular attention to the [specific topics identified in audit] addressed in the Access Control section of the NIST SP 800-53 guidance when documenting a policy governing and defining metrics."

Response:

GCOS concurs with this audit finding and we are currently working on developing a system-specific user access control policy and procedures for FOIAXpress.

U.S. Consumer Product Safety Commission Memorandum

TO: DeVaughn Moore, Auditor
Office of the Inspector General (OIG)

THROUGH: Stephanie Tsacoumis, General Counsel
Office of the General Counsel (OGC)

FROM: Alberta E. Mills
The Secretariat - Office of the Secretary
Office of the General Counsel (GCOS)

DATE: September 3, 2015

SUBJECT: The OIG's Final Set of Audit Findings for the FOIA Audit

GCOS has reviewed the final set of audit findings for the FOIA Audit and although we disagree with some of the conditions identified in the audit, we do agree that improvements to the FOIA Program would be beneficial.

Finding 1 – Fee Schedule

The OIG audit found that the fee schedule at CFR Title 16, Part 1015 does not include all of the required elements established by the FOIA Regulation. The audit recommendation states: "We recommend that GCOS management review and revise the CPSC published fee schedule and ensure the fee schedule is in line with current legislation. We also recommend that this schedule be reviewed periodically and updated as needed."

Response:

We concur with this audit finding. The fee structure at Title 16, Part 1015 was last updated in 1997. We agree that the fee schedule should be updated to reflect more current and accurate fee assessments. OGC will review and revise the fee schedule to include all required elements, will issue a Federal Register announcement to that effect and will periodically review and update the fee schedule. .

Finding 2 – Electronic Reading Room

The OIG audit found GCOS does not have a mechanism in place to determine frequently requested topics for posting on the FOIA webpage. The audit further found that the FOIA Electronic Reading Room is not updated in a timely manner and that the documents weren't properly indexed. The audit recommendation states: "We recommend GCOS develop guidance to determine subjects of frequent or subsequent request and timely perform updates to the Commission's electronic reading room."

Response:

GCOS will develop guidance, and establish and implement a mechanism, for determining frequently requested topics for posting on the FOIA webpage, and will timely update the FOIA Electronic reading room as recommended by the audit. GCOS also will review posted documents and documents to be posted in the future for proper indexing.

Note that CPSC's ability to make certain documents previously produced in response to a FOIA inquiry (such as incident reports and in-depth investigations) available on the FOIA webpage may be constrained by the statutory requirements of Section 6 of the CPSA.

Finding 3 – Statistical Reporting

The audit found that "GCOS management has not developed internal controls related to the development of the Commission's annual report to the Department of Justice" (DOJ). The audit recommendation states: "We recommend GCOS develop standard operating procedures to compile the annual report to the DOJ. These procedures should include a supervisory review to ensure the report's accuracy."

Response:

As recommended by the audit finding, GCOS will develop and implement internal controls that address the collection, maintenance and verification of FOIA-related information reported to DOJ. These internal controls will include written guidance and procedures for identifying communications that should be categorized as "FOIA requests" subject to FOIA processing and procedures. Written procedures also will address recordkeeping so that reliable and accurate information is collected and maintained regarding FOIA request received and processed.

The internal controls and procedures referenced in the preceding paragraph will include a requirement for supervisory review of the annual report to DOJ to ensure the accuracy of the information set forth in the report.

Finding 4 – FOIA Processing & Fee Assessments

The OIG audit found that "GCOS management has neither developed nor documented procedures to ensure that FOIA requests are properly completed or to adequately monitor the performance of the CPSC's FOIA program." The audit recommendation states: "We recommend the Chief FOIA Officer take more initiative monitoring the timeliness and completeness of completed FOIA requests. This should include:

- Tracking FOIA requests upon receipt to ensure they are completed within the statutory limit and receive the appropriate fee assessment;

- Performing an annual evaluation, with statistical benchmarks, of the CPSC's administration of the FOIA; and
- Develop, document and finalize policies and procedures over the CPSC's FOIA Program and ensure that they are consistent with the current FOIA legislation.

Response:

As recommended by the audit finding, GCOS will develop and document procedures to ensure that FOIA requests are properly and timely completed. Working with OGC, GCOS will develop, document and finalize policies and procedures governing the operation of the FOIA Program and will ensure that such policies and procedures are consistent with current FOIA legislation and regulations.

Such procedures also will provide for monitoring of the performance of the FOIA program. In particular, the Chief FOIA Officer will review timeliness and completeness of responses to pending and completed FOIA requests on a weekly basis and will provide periodic reports to OGC no less frequently than every two weeks. Further, the Chief FOIA Officer will perform and document an annual evaluation, with statistical benchmarks, of the CPSC's administration of FOIA.

The procedures to be adopted will call for entering FOIA requests into the tracking system on the same day of receipt and for the appropriate assessment of fees when applicable.

U.S. Consumer Product Safety Commission Memorandum

TO: DeVaughn Moore, Auditor
Office of the Inspector General (OIG)

THROUGH: Stephanie Tsacoumis, General Counsel ST
Office of the General Counsel (OGC)

FROM: Alberta E. Mills
The Secretariat - Office of the Secretary
Office of the General Counsel (GCOS)

DATE : March 27, 2015

SUBJECT: The OIG's Audit Findings for the FOIA Audit

GCOS has reviewed the audit findings for the FOIA Audit and agree with the recommendations suggested by the OIG's office. Following is our response to the findings.

Finding 1 - Untimely Update of the CPSC FOIA Directive

The OIG audit found that the CPSC FOIA Directive 0770.1 is outdated (last modification occurred in July 2006). The audit recommendation states: "We recommend that GCOS management review and revise the CPSC FOIA Program directive and related appendices to include current practices being performed and regulations established by the FOIA legislation. We also recommend that these directives be reviewed periodically and updated, as needed."

Response: We concur with this audit finding and will work with the Directives Coordinator to update the CPSC FOIA Directive 0770.1 to reflect the current practices of CPSC's FOIA program.

Finding 2 - FOIA Training

The OIG audit found that individuals charged with completing FOIA requests are not adequately trained in this endeavor. The audit recommendation states: "Develop and implement an annual training and development program for all agency employees involved with requests associated with the CPSC FOIA Program. The training should include education on the FOIA legislation, the CPSC's FOIA procedural requirements/internal controls an when and how to properly assess fees for FOIA records."

Response: We concur that FOIA training is vital to the CPSC FOIA Program. As a result GCOS will conduct an agency wide training for all staff and a more detailed training program for FOIA Specialists.

Finding 3 – Record Keeping

The audit found that "GCOS has not developed a proper method to track all FOIA requests received by the Commission that adheres to the NARA FOIA retention requirements." The audit recommendation states: "GCOS should either upload all FOIA requests received to the FOIAXpress system or create a systematic method of tracking FOIA Request and response that do not require electronic filing.

Response:

GCOS concurs with the finding that that our FOIA record keeping practice should be refined to properly account for all processed FOIA requests, whether they are entered into the official FOIA tracking system, FOIAXpress or maintained elsewhere.

Finding 4 – Lack of Internal Controls Over IDI Requests

The OIG found that the Clearinghouse "Program Analyst have not received the proper training on the application of FOIA legislation. Specifically, they have not received training on how to process FOIA requests over IDI report/files." The audit recommendation states: "Although the Clearinghouse is responsible for satisfying the FOIA requests for IDI files the CPSC's GCOS is ultimately responsible for the Commission's FOIA Program. Specifically this includes ensuring requests are received and processed in accordance with the FOIA legislation. Therefore we first recommend that the Program Analysts responsible for completing IDI requests in the Clearinghouse are included in the structured annual FOIA training program. The training should include education on the FOIA legislation, the CPSC's FOIA procedural requirements, and when and how to properly assess fees for FOIA records. Following the completion of the training, we recommend that the Clearinghouse with the assistance of GCOS develop a SOP to ensure that the receipt, processing, and tracking of FOIA requests for IDI files is accomplished in accordance with the FOIA legislation."

Response:

We concur that the Clearinghouse Program Analysts should receive annual FOIA training as with other agency staff. GCOS will also work with the Clearinghouse to develop a SOP for processing FOIA requests.