

United States
CONSUMER PRODUCT SAFETY COMMISSION
Bethesda, MD 20814

OFFICE OF INSPECTOR GENERAL

Consumer Product Safety Improvement Act Report to Congress

30 September 2013

TABLE OF CONTENTS

Executive Summary	1
Introduction	2
Assessment of the CPSC's Information Security Management	3
Assessment of the Third Party Laboratory Accreditation Program	8
Employee Complaints	15

Executive Summary

The Consumer Product Safety Improvement Act (CPSIA) of 2008 requires that the Office of Inspector General (OIG) of the U.S. Consumer Product Safety Commission (CPSC) include in an annual report to the appropriate congressional committees, the findings, conclusions, and recommendations from its reviews and audits performed under section 205 of the CPSIA. This year's report deals with the CPSC's capital improvement efforts involving information technology and the CPSC's laboratory accreditation program.

Capital Improvements: The CPSIA requires that the CPSC improve its information technology (IT) architecture in general. Last year's report dealt extensively with the CPSC's efforts to implement a structured IT investment management process. That will again be a focus of next year's report as a contract has been awarded to conduct a follow-up review of the CPSC's IT investment management process. However, this year's report focuses on the agency's efforts over the past several years to ensure the security of the information stored in the CPSC's IT systems.

The Federal Information Security Management Act (FISMA) requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency. It also requires that the relevant Office of Inspector General (OIG) perform an annual assessment of the agency's compliance with FISMA. The most recent available FISMA evaluation found that, although much work remains, management has made substantial progress in implementing the FISMA requirements.¹

Laboratory Accreditation Program Follow-Up Review: The CPSIA requires that the CPSC Office of Inspector General review the adequacy of procedures developed by the CPSC for accrediting conformity assessment bodies as authorized by section 14(a)(3) of the Consumer Product Safety Act (15 U.S.C. 2063(a)(3)), as amended by this Act.

The review conducted during this reporting period is a follow-up of the original review conducted over the CPSC's Third Party Laboratory Accreditation Program. The OIG's original review of the CPSC's laboratory accreditation program focused on the program's internal controls. It found that although CPSC management had done a remarkable job of creating a laboratory accreditation program out of whole cloth at the time field work was being done, there were still areas of the program that needed improvement. In particular, perhaps because of the rate at which the program was created, written policies and procedures often were found to be lacking; aspects of the review process appeared to be subjective; and internal control design was deemed weak in certain areas of the program's management. The follow-up review performed found that the agency had taken aggressive measures to address these findings.

¹ The FY 13 FISMA evaluation is currently underway, but the resulting report will not be issued until FY 14.

Introduction

This report has been prepared in accordance with the Consumer Product Safety Improvement Act (CPSIA) of 2008. The CPSIA requires that the Inspector General of the U.S. Consumer Product Safety Commission (CPSC) include in an annual report to the appropriate congressional committees, the Inspector General's findings, conclusions, and recommendations from the reviews and audits performed under subsections (a) and (b) of section 205 of the CPSIA. Those sections read as follows:

SEC. 205. INSPECTOR GENERAL AUDITS AND REPORTS.

(a) IMPROVEMENTS BY THE COMMISSION.—The Inspector General of the Commission shall conduct reviews and audits to assess—

(1) the Commission's capital improvement efforts, including improvements and upgrades of the Commission's information technology architecture and systems and the development of the database of publicly available information on incidents involving injury or death required under section 6A of the Consumer Product Safety Act, as added by section 212 of this Act; and

(2) the adequacy of procedures for accrediting conformity assessment bodies as authorized by section 14(a)(3) of the Consumer Product Safety Act (15 U.S.C. 2063(a)(3)), as amended by this Act, and overseeing the third party testing required by such section.

(b) EMPLOYEE COMPLAINTS.—Within 1 year after the date of enactment of this Act, the Inspector General shall conduct a review of—

(1) complaints received by the Inspector General from employees of the Commission about failures of other employees to enforce the rules or regulations of the Consumer Product Safety Act or any other Act enforced by the Commission or otherwise carry out their responsibilities under such Acts if such alleged failures raise issues of conflicts of interest, ethical violations, or the absence of good faith; and

(2) actions taken by the Commission to address such failures and complaints, including an assessment of the timeliness and effectiveness of such actions.

This report fulfills the above-referenced requirements.

Assessment of the CPSC's Information Security Management

The Federal Information Security Management Act (FISMA) requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency. It also requires that the relevant Office of Inspector General (OIG) perform an annual assessment of the agency's compliance with FISMA. Each year's FISMA evaluation both follows-up on the findings from the previous years and assesses the agency against any new standards developed. This year's FISMA evaluation found that, although much work remains, management has made substantial progress in implementing the FISMA requirements.² This evaluation was completed in accordance with the Quality Standards for Inspections issued by the Council of Inspectors General on Integrity and Efficiency's (CIGIE) Inspection and Evaluation Committee and not the Generally Accepted Government Audit Standards (GAGAS) issued by the Government Accountability Office.

The general theme of the findings was a lack of quality system reporting, in addition to, a lack of auditable evidence documenting the control activities performed by the resources responsible for the reviewed processes. These deficiencies, at least in part, resulted from a lack of adequate and up-to-date policies and procedures. Also contributing to the deficiencies identified was the lack of resources dedicated to implementing and enforcing the agency's documented policies and procedures throughout the Fiscal Year. Although management has updated many of the agency's IT security policies and improved several of their procedures, many improvements are still required. In addition, management did not disseminate these policies to all of the individuals/offices identified as having key procedural responsibilities.

The agency's system monitoring and reporting capabilities have substantially improved since FY 10. Management implemented several new tools in FY 11, and implemented a new IPS (Intrusion Prevention System) in FY 12. Although management has not fully optimized these tools, the system reporting possible now is far greater than it was a year ago and management has shown a commitment to continuing to improve the agency's system reporting capabilities. Management has also assigned an IT Security Specialist to the operations team to assist in the implementation and optimization of these tools.

Management has developed remediation strategies to address the known vulnerabilities, with a priority placed on the highest risk issues. The CPSC is in the process of remediating these issues. However, the full mitigation of these risks will require a significant amount of additional effort. For example, although the agency has still not fully implemented an effective Incident Response program, the CPSC has taken steps to remediate this issue. These steps include the establishment of a Computer Security Incident Response Team (CSIRT) to manage incidents. Management has also begun drafting detailed Standard Operating Procedures covering the incident response process, and management has begun to optimize the agency tool set to allow for the automatic identification and correlation of incidents.

² The report containing the results of the review upon which this portion of this report is based, as well as management's responses to same, may be found at the CPSC OIG webpage at <http://www.cpsc.gov/about/oig/oig.html>.

Another example of a remediation activity undertaken by CPSC management to eliminate existing vulnerabilities and improve overall system security is the continued improvement of the Continuous Monitoring Process. Although management has not fully implemented the Continuous Monitoring Plan, the security team is now providing monthly reports to senior management outlining the known risks to agency IT resources. This process will continue to improve as management optimizes its current tool set and improves system reporting. An effective Continuous Monitoring Process, once implemented, will result in the remediation of several other vulnerabilities, simply due to the improvements required in system reporting to facilitate the Continuous Monitoring strategy. The improvement in system reporting, in addition to the resulting analysis made possible by the enhanced reporting, will allow management to identify, quantify, and remediate weaknesses in other processes (such as Remote Access governance, Identity Management, and Security Incident Reporting) much more efficiently and effectively than is currently possible. This, in addition to the harmonizing of processes required for reporting, will result in a significant improvement in the overall system security.

Summary of Findings:

I. Security Management Controls

Prior Finding: Security management controls are enterprise-wide procedures for managing and assessing the risks and security controls of a system over its life cycle. CPSC management had not implemented sufficient management controls in the areas of risk management, review of security controls, life cycle management, authorized processing, and system security planning, as a result the techniques and concerns that are normally addressed by security management were not fully implemented. OMB Circular A-130, Appendix III requires sufficient management controls in these areas. This condition appears to have been due to the CPSC management not having the resources necessary to make the implementation of Security Management controls a priority.

Prior Recommendation: CPSC management should implement sufficient management controls in the areas of risk management, review of security controls, life cycle management, authorized processing, and system planning in order to ensure efficient and effective management of the IT system and its inherent risk.

Actions Taken: Management has made significant progress to address this issue, although gaps remain. Management is currently in the process of hiring an additional Information Systems Security Officer to assist with the oversight of IT security. The agency has also developed an SSP for each of the accredited major applications (CPSRMS and ITDSRAM) in addition to the GSS LAN. The agency contracted outside consultancies to perform independent security control assessments each year for the GSS LAN since NIST enacted the requirement in 2006, except for Fiscal Years 2006, 2009, and 2011. The agency has also developed and formalized, although not yet fully implemented, a policy and procedure for establishing a certification and accreditation process, which generally conforms to the required NIST Framework standards.

In FY 06, new security system requirements previously promulgated by NIST and OMB became mandatory. In order to retain accreditation and certification of their information systems, the CPSC was required to have its security controls independently tested and evaluated annually. Due to funding limitations, management did not do this in FY 06.

In order to meet the accreditation and certifications requirements outlined above, and to determine whether management correctly and effectively implemented the security controls identified for the GSS LAN in the SSP, during FY 07 the Office of Inspector General conducted a Security Test and Evaluation (STE Evaluation) in accordance with NIST SP 800-53. The STE Evaluation identified sixty-three (63) vulnerabilities for the CPSC General Support System. Of these, six were found to be high-risk vulnerabilities, 31 were found to be medium risk vulnerabilities, and 26 were found to be low risk vulnerabilities. The STE Evaluation Report included a planned mitigation with an associated due date for each vulnerability identified.

In FY 08, the CPSC regained system certification. Management accomplished this after the mitigation of the six high-risk vulnerabilities found in the STE Evaluation and the successful approval and testing of the CPSC's IT Contingency Plan.

In FY 09, a fundamental problem with the CPSC's Plan of Action and Milestones (POAM) was found. OMB has determined that agency POAMs must reflect known security weaknesses within an agency and, ". . . shall be used by the agency, major components, and program officials, and the IG as the authoritative agency management mechanism to prioritize, track, and manage all agency efforts to close security performance gaps." Although management had made changes in 2009 to help the agency address this shortcoming, the agency has not historically used a POAM as an affirmative management tool in addressing security weaknesses. Although it had historically done a good job of documenting known security weaknesses and prioritizing them, the agency had not used a POAM to either track or project the resources required or milestones necessary to address these weaknesses (as required by the OMB). As a result, the agency lacked historical data regarding its past efforts and failed to take advantage of a powerful planning tool in addressing current and future IT security challenges. Moreover, as of the conclusion of the FY 12 FISMA review, management still had not adequately implemented the POAM. Management did not document milestones and milestone dates for each of the known security weaknesses. Also, management did not reference the related capital investments for each of the security weaknesses identified in the POAM.

Our FY 09 review determined that the GSS LAN had maintained its certification and accreditation and that the system's security controls were, in the opinion of management, tested and reviewed in-so far as the agency continuously monitored the system. However, management had not updated or adequately tested the Contingency Plan in 2009, 2010, or 2011. Due to changes to the agency operating environment since the drafting of this plan, management decided that a new Information System Continuity Plan was necessary. To address this issue, management contracted an outside consultancy, Evoke, in FY 11 to draft Information System Contingency Plans (ISCP) for the GSS LAN and selected applications. Although management did not perform a functional test, as NIST requires, management performed a tabletop test of the GSS LAN ISCP, and documented the after-actions plans of the ISCP in November 2011. Now that management has drafted the GSS LAN ISCP, the agency is planning to complete a Business

Impact Analysis, establish an alternative processing site, and develop a Continuity of Operations Plan (COOP).

In FY 10, the CPSC contracted an outside vendor to perform and document the annual GSS LAN Risk Assessment, Security Test and Evaluation (ST&E), and Security Assessment Report (SAR), as well as to develop the SSP and to define a Continuous Monitoring process. This allowed the CPSC to identify risks, define compensating controls and outline remediation actions. The agency extended this contract in 2011 and 2012, and increased its scope to include the CPSRMS application. CPSRMS and ITDSRAM both obtained their security accreditation based on an independent security review of NIST requirements. CPSRMS obtained its accreditation in FY 11, and management reauthorized its security accreditation on October 3, 2012. ITDSRAM obtained its accreditation in FY 11. However, in FY 12, management did not have the ITSRAM application independently assessed for compliance with NIST requirements and did not formally reauthorize its security accreditation.

Also in FY 10 the Certification and Accreditation (C&A) policy did not define objective, measurable criteria that management could use to justify the certification and accreditation, recertification and reaccreditation, or conversely, decertification of an in-scope system. As of the FY 12 review, management still had not updated the policy. Furthermore, although the C&A policy addressed a process to continuously track changes to information systems that may necessitate reassessment of control effectiveness as defined by SP 800-37, management has not implemented a process to perform the security impact analyses necessary to perform these tasks.

2. Security Operational Controls

Prior Finding: Security operational controls are used to assess the security of the system processes and the people who interact with or operate those systems. Because CPSC management had not implemented sufficient operational controls in the areas of personnel security, data integrity, and documentation, CPSC management was not able to develop security procedures that focused on security mechanisms that affect the daily operation of the Commission. OMB Circular A-130, Appendix III requires that sufficient operational controls for personnel security, data integrity, and documentation be in place. This condition may have been due to the CPSC management not having the resources necessary to make implementation of operational controls a priority. The level of risk was rated "high" for personnel security and data integrity.

Prior Recommendation: CPSC Management should implement sufficient operational controls in the areas of personnel security, data integrity, and documentation in order to ensure efficient and effective management of the IT systems in support of the CPSC's mission.

Status at Time of Review: Significant progress has been made since 2001 to address this issue. The CPSC developed the Information System Security Plan (SSP) for the GSS LAN in 2002. Patriot, the contractor that developed the SSP, reported that in order for the CPSC to adequately implement and maintain the requirements of the SSP, a staff of three full-time personnel (information system security officer, network security engineer, and applications security engineer) would be needed. Qualifications for and responsibilities of each position were

delineated in the 2003 SSP. The CPSC has since hired an information system security officer and, in FY 11, provided him with one staff member to implement and maintain the SSP requirements. Management is also in the process of hiring a second information system security officer to oversee IT security. Management contracted out the remaining responsibilities on an "as needed" basis. However, management continues to require additional internal resources to adequately implement and maintain the SSP requirements.

In FY 2007, OMB mandated that agencies adopt security configurations for Windows XP and VISTA, as well as a policy for ensuring new acquisitions include common security configurations. (See OMB Memorandum M-07-11 "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems," and OMB Memorandum M-07-18 "Ensuring New Acquisitions Include Common Security Configurations") The CPSC has since formalized a Configuration Management Policy to govern this process. However, management had not fully implemented this policy, developed attendant procedures, or implemented configuration baselines for all agency hardware and software.

3. Security Technical Controls

Prior Finding: Security technical controls are specific to the system's ability to identify, track, and act on authorized or unauthorized usage. Because CPSC management had not implemented sufficient technical controls in the areas of identification and authentication, logical access, and audit trails, CPSC management had left sensitive information vulnerable. This condition appears to have been due to CPSC management not having the resources necessary to make implementation of sufficient technical controls a priority. The level of risk was rated high for identification and authentication, and logical access.

Prior Summary Recommendation: CPSC management should implement sufficient technical controls in the areas of identification and authentication, logical access, and audit trails in order to protect the information that is used to support the mission of the Commission.

Status at Time of Review: CPSC acknowledges its need for continued improvement. The CPSC has met the following goals in its effort to improve its security technical controls: implementing a security awareness training program, implementing solutions to perform automated system auditing, implementing the monitoring of Internet usage, implementing an Intrusion Prevention System, implementing multi-factor authentication for most agency resources, implementing a solution to restrict access to client USB ports by non-encrypted flash drives, implementing periodic reviews of user with elevated network privileges, and implementing a tool which allows the agency to inventory all network user accounts.

Assessment of the Third Party Laboratory Accreditation Program

To assess the adequacy of procedures for accrediting conformity assessment bodies as authorized by section 14(a)(3) of the Consumer Product Safety Act (15 U.S.C. 2063(a)(3)), as amended by the CPSIA, and to oversee the third party testing required by such section, this office conducted a review of the CPSC's Laboratory Accreditation Program.

Background: In relevant part, the CPSIA imposed a third-party testing requirement on all consumer products intended primarily for children 12 years of age or younger. Every manufacturer (including an importer) or private labeler of a children's product must have its product tested by an accredited independent testing laboratory and, based on the testing, must issue a certificate that the product meets all applicable Consumer Product Safety Commission (CPSC) requirements. The CPSIA gave the CPSC the authority to directly accredit third party conformity assessment bodies (hereafter referred to as "third party laboratories") to do the required testing of children's products or designate independent accrediting organizations to accredit the testing laboratories. The CPSC is required to maintain an up-to-date list of accredited laboratories on its website. The CPSC has authority to suspend or terminate a laboratory's accreditation, in appropriate circumstances, and is required to periodically assess whether laboratories should continue to be accredited. The third party testing and certification requirements for children's products are phased in on a rolling schedule. The statute requires the CPSC to issue laboratory accreditation regimes for a variety of different categories of children's products.

The OIG's review focused on two specific areas. First, it evaluated whether internal controls were designed adequately and executed properly in the management of the laboratory accreditation program. Second, it assessed the CPSC's compliance with the CPSIA in the operation of its conformity assessment program. This review was completed in accordance with the Quality Standards for Inspections issued by the Council of Inspectors General on Integrity and Efficiency's (CIGIE) Inspection and Evaluation Committee and not the Generally Accepted Government Audit Standards (GAGAS) issued by the Government Accountability Office.

The CPSC determined quickly that it lacked the necessary infrastructure to directly accredit the testing laboratories. So, to leverage its available resources, the CPSC used an independent accrediting organization to accredit the testing laboratories. The requirements for CPSC recognition include the following: (1) that the laboratory be accredited by a laboratory accreditation body that is a signatory to the International Laboratory Accreditation Cooperation (ILAC) Mutual Recognition Arrangement (MRA); (2) that the laboratory scope of accreditation include the test methods required by CPSC laws and regulations; and (3) that the laboratory apply to the CPSC for recognition and agree to fulfill the requirements of the CPSC program.

In implementing the CPSIA, in general, and the laboratory accreditation program, in particular, the CPSC faced challenges created not only by the requirement that it promulgate rules within mandatory timelines, but also by the complex scientific, technical, and procedural issues surrounding the rules. For example, the first in the series of rules dealing with laboratory accreditation (not a subject traditionally within the CPSC's jurisdiction) had to be promulgated within 30 days of the enactment of the CPSIA.

The CPSIA expanded the authority and the responsibilities of the CPSC. Prior to the passage of the CPSIA, the agency had never participated in the accreditation of laboratories, and had not been confronted with the daunting task of developing a program to accredit laboratories and overseeing their testing of certain consumer products. The CPSIA established an aggressive regulatory agenda and set deadlines to ensure that results were achieved in a timely fashion. The vigorous requirements of the CPSIA have had positive as well as negative effects on the agency. The CPSIA has spurred a greater degree of regulatory activity. Meanwhile, it established implementation deadlines requiring the CPSC to move at a pace that it has not always been able to achieve.

Summary of Findings: The OIG found that although the CPSC has done a remarkable job of creating a laboratory accreditation program out of whole cloth at a time when field work was ongoing, there were other areas of the program that needed improvement. Initially, perhaps because of the rate at which the program was created, written policies and procedures often were lacking; certain aspects of the review process appeared to be subjective; and internal controls design was weak in certain areas of the program's management. The follow-up review found that the agency had taken aggressive measures to address a number of the findings detailed in the original report. Summaries of the specific findings made in the OIG's report are set forth below.³

Initial Finding 1. No Published Methodology or Detailed Criteria Developed for Evaluation of Government Laboratories

We found that there was neither a published methodology nor detailed criteria established for the evaluation of government laboratories. The criteria for evaluating third-party and firewalled laboratories were spelled out fairly clearly and made available to the public on the CPSC's website. However, no such criteria have been published for government-controlled laboratories, and it appeared that no such criteria existed, at least in a written form.⁴

As a result of the apparent lack of criteria, the evaluation of government laboratories may appear subjective. This appearance of subjectivity could increase the chances that an unsuccessful applicant would challenge the agency's decision to deny accreditation.

Recommendation: Develop a baseline or minimum set of documents and requirements that government laboratories must meet to be accredited; continue to use the current multi-person panel to evaluate applications to reduce subjectivity.

Actions Taken by Management to Implement Recommendation: The CPSC has developed a standard set of questions and requests for documentation that it uses for all governmental lab

³ The report containing the results of the review upon which this portion of this report is based, as well as management's responses to same, may be found at the CPSC OIG webpage at <http://www.cpsc.gov/about/oig/oig.html>.

⁴ The CPSIA establishes the underlying criteria to be evaluated (e.g., the existence of "undue influence"), but not how that evaluation should take place (e.g., independent investigation, information provided by other federal agencies).

applicants. Requests for information from U.S. missions abroad also now utilize standard language. All applicants are reviewed using a standardized review document that provides grounds and reasoning for a finding relative to each of the five criteria for governmental labs set forth in the statute. The agency reports that all EXIP staff have been trained in the standard procedures, but that this training is not formally documented. **Recommendation Closed**

Initial Finding 2. No Policies or Procedures Developed to Audit Third Party Laboratories as Condition of Continuing Accreditation

The CPSIA requires that no later than 10 months after the date of enactment of the CPSIA, the CPSC, by regulation, should establish requirements for the periodic audit of third party laboratories, as a condition of the continuing accreditation of such bodies. This requirement was to be completed by June 2009.

The CPSC does not have written policies or procedures in place to audit third party laboratories. As a result, the CPSC has no way of verifying whether the third party laboratories that it has accredited previously currently are complying with the accreditation requirements.

Recommendation: The CPSC should develop and implement written policies and procedures for auditing third party laboratories.

Actions Taken by Management to Implement Recommendation: The agency has published a proposed rule to formally establish policies and procedures for the audit of third party laboratories. This proposed rule, 16 CFR Part 1112 was published on May 24, 2012.
Recommendation Closed

Initial Finding 3. Inadequate Monitoring of Certification Expiration Dates

In accordance with section 102(e)(1)(B) of the CPSIA, the CPSC may withdraw its accreditation or its acceptance of the accreditation of a third party laboratory if the CPSC finds such laboratory failed to comply with an applicable protocol, standard, or requirement established by the CPSC.

However, the CPSC does not have written procedures to monitor whether certifications have expired certifications or whether certificates are up for renewal. Instead, the CPSC conducts follow-up checks— which are not documented or recorded—on an *ad hoc* basis.

The lack of documented procedures for monitoring certificate expiration dates increases the risk that an unauthorized laboratory will continue to be recognized as an accredited laboratory by the CPSC.

Recommendation: The CPSC should develop and implement procedures for regularly monitoring certification/certificate renewals and detecting expired certifications and maintain records of these reviews. Laboratories with expired certifications should be removed from the accredited laboratory list maintained electronically by the CPSC.

Actions Taken by Management to Implement Recommendation: The CPSC has developed an internal standardized operating procedure for both monitoring certification/certificate renewals and detecting expired certifications on a regular basis. They also now maintain records of these reviews. A standardized policy has also been developed for removing laboratories with expired certifications from the CPSC maintained accredited laboratory list after it has been confirmed that they have had their accreditation suspended or removed by their accreditation body. **Recommendation Closed**

Initial Finding 4. No Written Policies or Procedures Exist for Removing Third Party Laboratory's Certification.

The CPSIA contemplates two situations that may lead to the withdrawal of a third party laboratory's certification. First, in accordance with CPSIA, Section 102(e)(1)(A), the CPSC may withdraw its accreditation or its acceptance of the accreditation of a third party laboratory if the CPSC finds that a manufacturer, private labeler, or governmental entity has exerted undue influence on such conformity assessment body or otherwise interfered with or compromised the integrity of the testing process with respect to the certification of a children's product. Second, CPSIA, Section 102(e)(1)(B) states that the CPSC may withdraw its accreditation or its acceptance of the accreditation of a third party laboratory if the CPSC finds such laboratory failed to comply with an applicable protocol, standard, or requirement established by the CPSC.

The CPSC does not have written policies or procedures to address the requirements of CPSIA, Section 102(e)(1)(A) or (B).

As a result, its process of withdrawing accreditation is not standardized, leaving the agency subject to a claim in court that it acted in an arbitrary and capricious manner when it withdraws accreditation from a laboratory. It is unclear what policies and procedures the CPSC will implement to withdraw recognition or acceptance of a third party laboratory's accreditation.

Recommendation: The CPSC should develop and implement written policies and procedures for withdrawing a third party laboratory's certification.

Actions Taken by Management to Implement Recommendation: The agency has published a proposed rule to formally establish policies and procedures for the withdrawing of a third party laboratory's certification. This proposed rule, 16 CFR Part 1112 was published on May 24, 2012. **Recommendation Closed**

Initial Finding 5. No Written Policies or Procedures Exist for Reviewing Employee Training Records Contained in Firewalled Laboratory Accreditation Application Packages

In addition to the baseline accreditation requirements, firewalled laboratories must submit in English, copies of their training documents to the CPSC. These documents should demonstrate that the laboratory's employees have been trained to understand that they may notify the CPSC

immediately and confidentially of any attempt by a manufacturer, private labeler, or other interested party to hide or exert undue influence over the third party laboratories' test results. This additional requirement applies to any third party laboratory in which a manufacturer or private labeler of a children's product to be tested by the third party laboratory, owns an interest of 10 percent or more in the laboratory in question.

No written policies or procedures exist on how to implement the above-described requirements. During field work, we observed that there was little standardization or uniformity in the evaluation process. As a result, there is a lack of consistent enforcement or implementation of application requirements. For example, not all application packages examined contained the actual signatures of the employees who allegedly attended the training. The lack of employees' signatures on the training attendance list increases the difficulty of establishing whether the listed attendees actually received the training in question.

Recommendation: Develop and implement written policies and procedures to describe what constitutes acceptable training documents and related minimum requirements for firewalled laboratory application packages.

Actions Taken by Management to Implement Recommendation: The agency has published a proposed rule, 16 CFR Part 1112, to formalize the requirement that conformity assessment bodies that apply for CPSC approval as firewalled laboratories must submit to the Commission copies of their training documents, showing how employees are trained to notify the Commission immediately and confidentially of any attempt by the manufacturer, private labeler, or other interested party to hide or exert undue influence over the third party conformity assessment body's test results. This proposed rule also contains descriptions of what constitutes acceptable training documents. **Recommendation Closed**

Initial Finding 6. CPSC Failed to Meet Number of Accreditation Timeline Requirements

The CPSIA and related regulations created a number of timeline requirements for the establishment of accreditation requirements. The accreditation requirements for baby bouncers, walkers, and jumpers were to be established not later than 210 days after enactment of the CPSIA, or March 12, 2009. All other current CPSC children's product safety rules were to be created not later than 10 months after enactment of the CPSIA, or June 14, 2009). The CPSIA also required the CPSC to establish, by regulation, requirements for the periodic audit of third party laboratories, as a condition of the continuing accreditation of such bodies. The periodic audit requirement was supposed to be met not later than 10 months after the date of enactment of the CPSIA, June 14, 2009.

The CPSC did not publish *Federal Register* notices of accreditation requirements for baby bouncers, walkers, and jumpers by March 2009, as required by the CPSIA timeline.

Of the five classes of children's products mentioned specifically in the CPSIA regulation, four of the classes successfully met the timeline requirements, and only one class (baby bouncers, walkers, and jumpers) did not post before the required timeline expired. The rule for infant

walkers finally posted to the *Federal Register* in June 2010, 15 months after the CPSIA timeline required.

There does not appear to be a predominate reason for the agency's failure to meet certain required timelines set forth in the CPSIA. In the case of baby bouncers, walkers, and jumpers, staff indicated the desire to produce a "better" rule than the previous rule. In the case of auditing third party laboratories, staff completed other projects demanding more immediate attention.

Recommendation: Increase the emphasis on meeting congressional mandates.

Prior Management Response: The CPSIA represents the most substantial change in consumer product safety since the creation of the Agency in 1973. Since August 2008, CPSC staff has worked diligently to implement the CPSIA through rulemaking, enforcement, and other safety standard activities. In 2010 we have completed over 30 rules or other documents required by the CPSIA. The number of completed assignments required by the CPSIA, however, is only a partial accounting of Commission staff's actual workload. For example, in some cases, a statutory requirement under the CPSIA triggered additional work and the need for the Commission staff to issue a proposed rule (before it could issue the CPSIA required final rule), an interpretive rule, a statement of policy, or a guidance document. These other rules and documents constitute an additional 50 items completed since August 2008 (20 items completed in 2009, 30 items completed in 2010). We also held numerous public briefings to help stakeholders understand their obligations under the law, created a special Web site devoted to CPSIA, and responded to thousands of inquiries from affected manufacturers, retailers, resellers, and consumers.

At the same time the CPSC was working on the implementation of the CPSIA it was called upon to deal with two other challenges. Staff resources had to be reallocated to work on the unplanned and unbudgeted drywall problem and in December 2008, the Virginia Graeme Baker Pool and Spa Safety Act (Pool and Spa Safety Act) became effective. In working to implement the Pool and Spa Safety Act CPSC staff participated in Webinars, held meetings, and disseminated information on the Pool and Spa Safety Act to all pool and spa owners, operators, technicians, manufacturers, state and local health officials, and other organizations concerned with children's safety and drowning. CPSC staff inspected over 1,200 public pools and spas in 38 states for compliance with drain cover requirements of the Act. We also entered into a partnership with the Centers for Disease Control to provide states in 2010 with enforcement grants and funded a major information campaign to begin in 2010.

The CPSC did not publish a notice of requirements pertaining to walkers, bouncers, and jumpers in 2009 because, at the time, staff intended to revoke the regulation (see "Revocation of Regulation Banning Certain Baby-Walkers and Similar Products," 74 FR 45714 (September 3, 2009)) and issue a new standard for walkers. However, after publication of the proposed rule to revoke the regulation, CPSC staff reconsidered their position and elected to revoke only those aspects of the rule pertaining to walkers. The issuance of a final rule establishing a new standard for walkers was accompanied by a notice of requirements for walkers ("Third Party Testing for Certain Children's Products; Infant Walkers; Requirements for Accreditation of Third Party Conformity Assessment Bodies," 75 FR 35282 (June 21, 2010)), and CPSC staff intends to issue

a notice of requirements pertaining to bouncers and jumpers when it develops final standards for those products.

Actions Taken by Management to Implement Recommendation: The overall pace at which the agency has issued notice of requirements and met other mandates has accelerated since the passage of the CPSIA. FY 11 saw over 13 notices of requirement issued by the CPSC become effective, to include those relating to infant walkers and final rules formalizing the implementation of many of the CPSIA's requirements have recently been implemented. FY 12 also saw an increased emphasis in this area, however given the procedural requirements and resource challenges facing the agency, it is possible that the agency will not be able to comply with the required timetable for rulemaking in the near future. **Ongoing**

Initial Finding 7. Overreliance on ILAC to Ensure Laboratories Conform to CPSIA Standards

At the time fieldwork was conducted, the CPSC was relying nearly exclusively on ILAC to ensure that the laboratories accredited by the CPSC actually conformed to CPSIA standards.

Although the CPSIA (Section 102(a)(1)(3)(C)) does permit the CPSC to accredit third party laboratories directly or through an independent accreditation organization, concerns exist about whether the CPSC demonstrated adequately and documented completely— prior to the agency opting for ILAC as the independent accreditation organization—that ILAC standards/test methods conform to CPSIA standards.

Based upon our findings, it appears that the CPSC may be relying too heavily on ILAC's accreditation process to determine whether to accredit laboratories as CPSIA compliant. It appears that tight deadlines and other resource constraints may be contributing factors in the CPSC's reliance on ILAC accreditation.


Recommendation: Consider conducting field visits or onsite inspections or employing some other monitoring mechanism to verify the validity and quality standards of third party laboratories. Perform these visits randomly, or when concerns arise, to limit reliance on ILAC certification.

Prior Management Response: The IG recommendation to conduct field visits/onsite inspections to "limit reliance on the ILAC certification" is noted and considered an appropriate action for CPSC to take, as circumstances dictate.

Actions Taken by Management to Implement Recommendation: The CPSC has begun conducting site visits at accredited laboratories to "limit reliance on the ILAC certification." However, the ability of the CPSC to carry out such visits on a large scale is severely limited by the resources available. To date, there has been no formal documentation of or guidance issued on conducting these site visits. **Ongoing**

Employee Complaints

No complaints fitting the definitions set forth in section 205(b) of the CPSIA have been filed with this office.



Christopher W. Dentel
Inspector General
U.S. Consumer Product Safety Commission