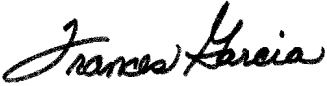


# Memorandum

**Date:** November 15, 2012  
**To:** The Honorable Commissioners  
**From:** Frances Garcia, Inspector General   
**Subject:** Fiscal Year 2012 Federal Information Security Management Act Evaluation

We have completed an independent evaluation of the effectiveness of the United States Commission on Civil Rights' (USCCR) information security program and practices for fiscal year 2012 as prescribed by the Federal Information Security Management Act of 2002 (FISMA).<sup>1</sup> FISMA requires federal agencies to develop, document, and implement an agencywide information security program to provide security for the information and information systems that support their operations and assets, including those provided or managed by another agency, contractor, or other source. In addition, this act requires each agency to report annually on their information security programs to the Office of Management and Budget (OMB). Further, each agency is required to have an annual independent evaluation of its information security program and practices, including control testing and compliance assessment, which is to be performed by the agency Inspector General (IG) or by an independent external auditor.

The Consolidated and Further Continuing Appropriations Act of 2012 designated that the Government Accountability Office (GAO) IG holds the position of USCCR IG and directed that personnel from GAO's Office of Inspector General (OIG) be utilized to perform the duties of USCCR IG. This is the first FISMA review we have performed. As a result, there were no prior USCCR IG recommendations to follow up on.

Our evaluation showed that USCCR has established an overall information security program that is generally consistent with the requirements of FISMA, OMB implementing guidance, and standards and guidance issued by the National Institute of Standards and Technology (NIST). However, we did identify improvements needed for elements of this program that concern contingency planning, configuration and vulnerability management, risk management, and security training. This report includes recommendations to help the agency more fully implement federal information security requirements for these program elements. (See Attachment.)

---

<sup>1</sup>Enacted as Title III of the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).

The objectives of our evaluation were to assess (1) the effectiveness of USCCR's information security policies, procedures, and practices; and (2) USCCR's compliance with FISMA information security requirements and other federal information security policies, procedures, standards, and guidelines. We focused our work on USCCR's implementation of required information security program elements and practices as reflected in IG reporting metrics for fiscal year 2012, provided by the Department of Homeland Security.<sup>2</sup> These metrics address 11 information security areas: (1) Continuous Monitoring Management, (2) Configuration Management, (3) Identity and Access Management, (4) Incident Response and Reporting, (5) Risk Management, (6) Security Training, (7) Plan of Action and Milestones (POA&M), (8) Remote Access Management, (9) Contingency Planning, (10) Contractor Systems, and (11) Security Capital Planning. To assess USCCR's performance for these areas, we analyzed its information security policies and procedures and determined the extent to which specific security requirements were implemented. We also considered an external auditor's work on USCCR's biennial assessment of information security and incorporated the results into our evaluation as appropriate.<sup>3</sup>

We conducted this evaluation from September 2012 to November 2012 in accordance with the quality standards established by the Council of the Inspectors General on Integrity and Efficiency. Those standards require that we plan and perform the evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our evaluation objectives.

### **Agency Comments**

The IG provided USCCR with a draft of this report for review and comment. USCCR agreed with our recommendations and provided no technical comments.

Actions taken in response to our recommendations are expected to be reported to my office within 60 days.

If you would like to discuss these conclusions and recommendations please contact me at (202) 512-5748 or [garciaf@gao.gov](mailto:garciaf@gao.gov).

---

<sup>2</sup>U.S. Department of Homeland Security, *FY 2012 Inspector General Federal Information Security Management Act Reporting Metrics*, (Mar. 6, 2012).

<sup>3</sup>NucoreVision Incorporated, *Assessment of USCCR Information Security & Assurance Program as it Relates to FISMA Requirements inclusive of Inspector General Response*, (Lanham, MD: Nov. 9, 2012).

*List of Addressees*

The Honorable Martin R. Castro, Chairman

The Honorable Abigail Thornstrom, Vice Chair

The Honorable Roberta Achtenberg

The Honorable Todd Gaziano

The Honorable Gail Heriot

The Honorable Peter Kirsanow

The Honorable David Kladney

The Honorable Michael Yaki

## Attachment

### Improvements Are Needed to Fully Implement Security Program

Our overall evaluation showed that the United States Commission on Civil Rights (USCCR) has established an information security program that is generally consistent with federal requirements, guidance, and standards. However, in evaluating elements of this program based on the Department of Homeland Security's reporting metrics for Inspectors General (IG), we identified specific improvements needed to help ensure that security requirements are fully implemented. Evaluation results for these program elements are as follows.

#### Limitations Exist in Information Technology Contingency Planning

USCCR maintains an overall continuity program, which, among other things, provides for the health and safety of USCCR employees, contractors, and visitors, and helps ensure that USCCR will be able to maintain its operational capability in the face of significant threats. As a key element of this program, USCCR maintains a Continuity of Operations Plan (COOP) that:

- identifies essential agency functions, vital records, and critical systems;
- assigns roles and responsibilities, orders of succession, and delegations of authority for USCCR staff; and
- describes the activation of the COOP, relocation to an alternate site, and resumption of operations once the emergency or other event has concluded.<sup>4</sup>

This plan covers business operations and systems owned or maintained by USCCR, which is responsible for their continuity of operations. However, this plan does not cover hosted systems on contractor or other government networks, such as the USCCR's electronic mail, document management, and publicly-accessible websites, that are the responsibility of each respective service provider.

While USCCR has taken steps to sustain the agency's essential functions and provide continuity of operations in the event of a disruption, USCCR has never performed testing, training, and exercises to validate the effectiveness of the USCCR continuity program. According to NIST, testing is a critical element of a viable contingency capability. Testing enables plan deficiencies to be identified and addressed by validating one or more of the system components and the operability of the plan. Testing can take on several forms and accomplish several objectives but should be conducted in as close to an operating environment as possible. Training for personnel with contingency plan responsibilities should be conducted annually to ensure that the staff is prepared for an emergency or other event. Finally, exercises are the simulation of an emergency designed to validate the viability of one or more aspects of a continuity program. In an

---

<sup>4</sup>USCCR, *Continuity of Operations Plan*, (June 2010).

exercise, personnel validate the content of a plan through discussion of their roles and their responses to emergency situations, execution of responses in a simulated operational environment, or other means of validating responses that do not involve using the actual operational environment.

### Configuration and Vulnerability Management Weaknesses Increase Security Risk

Our evaluation showed that USCCR has a process for configuration management that includes baseline configurations and hardening guidelines.<sup>5</sup> However, during the biennial assessment in 2012, vulnerability scans by an external auditor identified numerous vulnerabilities that pose a significant risk to information systems used and accessed by USCCR. Further, USCCR cannot fully remediate these configuration-related weaknesses and vulnerabilities due to the technological limitations of outdated computers. While USCCR plans to replace this equipment by February 2013, these weaknesses currently represent a risk for USCCR's information systems and the operations they support.

USCCR also does not have a written configuration management policy. The Federal Information Security Management Act (FISMA) requires that federal agencies' information security programs include policies and procedures to ensure compliance with minimally acceptable system configuration requirements. A well-defined configuration management policy and process that integrates information security is needed to ensure that the security of an information system or the organization is not adversely affected by change. For example, adjustments to a system's configuration may be required as a result of new, enhanced, corrected, or updated hardware and software capabilities; patches for correcting software flaws and other errors to existing components; or new security threats or changing business functions.

### USCCR Lacks Risk Management Framework and Policy for Information System Security

USCCR has implemented security measures and controls that primarily address security risks for individual information systems. This approach includes ad-hoc processes for the selection and implementation of security controls and continuous monitoring or periodic assessment of these controls. However, it does not address information security risks from an overall agency perspective through a comprehensive formal governance structure and organization-wide risk management strategy, as prescribed by NIST guidance.

---

<sup>5</sup>A baseline configuration is a set of specifications for a system that has been formally reviewed and agreed on at a given point in time and that can be changed only through change control procedures. A "hardening guide" is a security configuration checklist that helps organizations to automatically set and verify the appropriate security settings for different information technology products.

According to the Deputy Chief Information Officer (CIO),<sup>6</sup> the USCCR does not have a formal Risk Management Framework or written policy on risk management. During our evaluation of the risk management process, we also determined that the Deputy CIO did not brief the Commissioners on specific risks and threat activity. We believe such briefings are important in establishing and maintaining an organization-wide risk management strategy for information security.

A Risk Management Framework emphasizes building information security capabilities into federal information systems through the application of state-of-the-practice management, operational, and technical security controls; and maintaining awareness of the security state of information systems on an ongoing basis through enhanced monitoring processes. In addition, the framework provides essential information to senior leaders to facilitate decisions regarding the acceptance of risk to organizational operations and assets, individuals, other organizations, and the nation, arising from the operation and use of information systems.<sup>7</sup>

#### Policies and Procedures to Ensure Security Training Compliance Should Be Improved

Our evaluation determined that USCCR does not have effective policies and procedures to ensure all staff with network access receive annual information security awareness training, as required. USCCR has procured information security training support to provide (1) annual information security awareness training for USCCR employees and contractor staff with network access, and (2) role-based information security awareness training for those with specialized responsibilities. For fiscal year 2012, the training was available online, but the Deputy CIO maintained hard-copy files to help show the extent to which USCCR complied with these training requirements. We created a list of 44 users as of September 30, 2012, by reviewing network documentation and the September 2012 staff directory and staff roster. Of those 44 users, 17 (39 percent) had a certificate on file to document completion of annual information security awareness training in fiscal year 2012. The remaining 27 users (61 percent) did not have a certificate on file. This included Commissioners and Regional Staff that have access to USCCR electronic mail and shared documents but were not included in the process to ensure completion of annual information security awareness training.

---

<sup>6</sup>The Deputy CIO is responsible for information security and enterprise architecture. There is not currently a CIO for the USCCR.

<sup>7</sup>NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems*, Special Publication 800-37 Revision 1 (Gaithersburg, MD; February 2010).

## **Conclusions**

It is essential to ongoing program effectiveness that USCCR continually assess whether established processes and practices are operating as intended and make certain that changes in federal security requirements, guidance, and techniques are proactively incorporated into a formal, well-documented program. In addition, senior management involvement in determining how the organization assesses and mitigates information system-related security risks will help to strengthen the agency's overall information security program.

## **Recommendations for Executive Action**

To help strengthen USCCR's overall information security program, we recommend that the Deputy CIO take the following five actions:

- (1) Conduct COOP testing, training, and exercises to validate the effectiveness of USCCR continuity program.
- (2) Ensure the timely remediation of vulnerabilities due to outdated equipment.
- (3) Create a written configuration management policy to ensure compliance with minimally acceptable system configuration requirements.
- (4) Develop and provide for USCCR senior management consideration a proposed approach for establishing a comprehensive governance structure and organization-wide risk management strategy for information system security that would include a process for keeping management apprised of specific risks and threat activity.
- (5) Develop and implement policies and procedures for ensuring all staff with network access complete information security awareness and role-based training requirements as of the end of each fiscal year reporting period.

(999824)

### **Reporting Fraud, Waste, and Abuse in the U.S. Commission on Civil Rights**

To report fraud, waste, or abuse in Commission programs and operations, do one of the following. (You may do so anonymously.)

- Call toll-free (866) 680-7963 to speak with a hotline specialist, available 24 hours a day, 7 days a week.
- Report online at: <https://oig.alertline.com>.

### **Obtaining Copies of Office of the Inspector General Reports, Publications, and Testimonies**

Copies of OIG reports, publications, and testimonies are available on the Commission's website: <http://www.usccr.gov/OIG/index.php>.