UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, DC 20436

December 05, 2013 OIG-ML-14-04 IG-LL-020

Commissioners,

The Commission submitted its Annual Federal Information Security Management Act (FISMA) report on December 2, 2013. The report contains more than 100 questions about the information security program here at the USITC. We answered 48 of the questions with a "no," meaning that the program is missing 48 components. The Chairman requested we prepare this Management Letter to explain the implications for the USITC and what actions can be taken to improve information security.

The FISMA report assesses the maturity of an agency's information security program; it covers a wide range of program components. As with managing any task, it is important to focus on doing the right work and to handle the most important things first. Because of the large number of "no" answers; I am concerned that the Commission may focus on too many things and not on the *most important* things. Guidance from DHS (Attachment 1) identifies the twenty most important security controls, the top four of which are the *only* controls rated as "very high" for the mitigation of attacks by the National Security Agency (NSA).

These controls are:

1. Inventory of Authorized and Unauthorized Devices:
    - **Know the devices on your network.**
2. Inventory of Authorized and Unauthorized Software:
    - **Know the software on your network.**
3. Secure Configurations for Hardware & Software on Laptops, Workstations, and Servers:
    - **Secure systems by default.**
4. Continuous Vulnerability Assessment and Remediation:
    - **Monitor and patch continuously.**

The Office of Inspector General has audited each of these areas, including patch management, which was the subject of our latest report (Attachment 2). This report identified that the Commission did not have an effective patch management program. The data from this report was the basis for many of the "no" answers on the FISMA report, and demonstrated that the Commission was not implementing the four critical controls. Therefore the Commission is not effectively managing the information security of its network.

To assure the security of its network, the Commission should focus on the top four NSA Critical Controls.

Regarding the first control, we issued a recommendation in our recent patching audit report, "That the CIO shrink the network to facilitate at least weekly patch scanning of all hosts." This recommendation is pending a management decision. Note that the OIG first made this recommendation in a 2011 audit report. (Management decided to not implement this recommendation.)

For the second control, the most effective means to manage the software on a network is through use of a technology known as "white listing" which determines the specific software that is permitted to run on a network, and denies all other software from being executed. Therefore, we recommend the following:

Recommendation 1: The Commission implement whitelisting to prevent unauthorized software from running on the network.

The third and fourth controls would be implemented by effective management decisions that adopt the remaining six recommendations made in the OIG *Audit of the Commission's Patching Process*.

Having these four controls in place will allow the Commission to act on the November 18th, 2013, OMB memorandum, *Enhancing the Security of Federal Information and Information systems*. (Attachment 3) The purpose of this memorandum is to shift the focus of government security reviews from a static "once every three years" process to one that consistently assesses and fixes security issues. Specifically OMB wants agencies to focus attention on "what data and information are entering their networks, who is on their systems, and what components are on their information networks as well as when their status changes."

Implementing these OIG recommendations will help the USITC focus on the critical controls for information security. The process of automating these controls will go a long way toward building the program discussed in the FISMA report. Demonstrated effectiveness of these controls will provide you with confidence that your information security program is built on a solid foundation.

Philip M. Heneghan
Inspector General, USITC

List of Attachments:

Attachment 1: DHS co-sponsored poster of 20 Critical Security Controls (SANS Institute)

Attachment 2: OIG Report: *Audit of Patch Management Process*

Attachment 3: Enhancing the Security of Federal Information and Information systems