OFFICE OF INSPECTOR GENERAL

MEMORANDUM

DATE: March 28, 2000

TO: Chairman

FROM: Inspector General

SUBJECT: Report on Special Review of Auctions Security

The Office of Inspector General (OIG) has completed a Special Review of computer security on the Commission's Auction sub-network. A copy of our final Special Review Report, entitled "Report on Special Review of Auctions Security" [Assignment No. 00-AUD-01-21], is attached. A special review is meant to be a quick study of a process and, as such, was not conducted in accordance with all professional auditing standards.

The OIG initiated this special review to investigate a referral by the Commission's Computer Security Officer. On October 1, 1999, the Computer Security Officer sent an e-mail message to the Inspector General informing the Inspector General of an unexplained access to a key user account on the Auctions sub-network. Based upon the initial reports of potential system compromise, the OIG responded by initiating a task order under our contract with the computer security firm of TWM Associates, Inc. (hereafter referred to as "TWM") and establishing a review team comprised of representatives from TWM and the OIG. The primary objective of the investigative portion of the special review was to determine specifically what took place and, to the extent that this information could be developed, who was inappropriately using a privileged account on the Auctions sub-network. Following discussions with Auction and Information Technology Center (ITC) personnel and security tests of components of the Information Technology (IT) environment, the OIG review team concluded that the specific incident triggering this investigation appears to have been the result of a database system security feature and not a malicious attack. A Flash Report, entitled "Flash Report on the Results of the Preliminary Investigation of the Auction Sub-network Security Incident", summarizing the preliminary investigative portion of the review was issued on October 12, 1999 and is included as Appendix A in this report.

A secondary objective of the special review was to evaluate the security of the Auctions sub-network technology to determine if security improvements can be made and to examine the incident reporting process followed in this case to determine if the process was appropriate given the facts of the case. During the second phase of the review, the review team identified findings

covering the administration of the Auctions systems and the technology employed by the Auctions site. The administrative findings focus on the plans, policies and procedures in place to ensure that the systems in question are administered in a secure manner. Our review determined that, in general, the plans, policies and procedures in place over the Auctions system need improvement. In addition, our review indicates that adherence to the existing plans, policies and procedures was not sufficient to ensure adequate security for the Auctions system. The review team made several recommendations to strengthen existing plans, policies, and procedures. The technology-based findings focus on the secure implementation and deployment of technology within the system. The review identified lack of adherence to password standards within Unix and the Auctions application; auditing was not sufficiently configured at the network and application levels to ensure accountability; and excessive permissions exist on system objects. The specific findings identified during this review are summarized in the section of the Special Review Report entitled "Review Findings." A detailed description of the specific findings and a matrix of the detailed findings are included in Appendices B and C, respectively.

The Wireless Telecommunications Bureau (WTB) provided a response to preliminary review findings on November 10, 1999 and a formal response to the Draft Special Review Report on January 28, 2000. The Office of Managing Director (OMD) responded to the Draft Special Review Report on February 9, 2000. Based on those responses and subsequent discussions, OMD and WTB ultimately indicated concurrence with forty-two (42) and non-concurrence with two (2) of the forty-four (44) findings. We have incorporated each OMD/WTB response by finding into the detailed description of each finding contained in Appendix B of the report and, in those cases where it was appropriate, we have provided comments to the OMD/WTB responses. In addition, we have included a complete copy of each WTB and OMD response in Appendices G, H, and I respectively. Because of the sensitive nature of the information contained in the appendices to this report, we have watermarked these appendices "Confidential" and have distributed copies only to those personnel with a need for the information. Those persons receiving this report are requested not to photocopy or otherwise distribute this material.

We would be happy to meet with you to discuss the results of this special review. If you have any questions, please contact me at 418-0476.

for H. Walker Feaster III

Attachment

CC: Chief of Staff
Chief, Wireless Telecommunications Bureau
Managing Director
AMD – PERM (with appendices)
Director Technical Operations, WTB - Auctions and Industry Analysis Division (with appendices)
Computer Security Officer (with appendices)