Federal Communications Commission
Office of Inspector General

Report on Audit of the Automated Auction System (AAS)

Audit Report No. 02-AUD-02-08
June 28, 2002

H Walker Feaster
H. Walker Feaster III
Inspector General

Thomas D. Bennett
Assistant Inspector General – Audits

Walter P. Opaska
Walter P. Opaska
Director – IS Audits

TABLE OF CONTENTS

Executive Summary

The Automated Auction System (AAS) is a major application system which is responsible for processing all Federal Communications Commission (FCC) spectrum auctions. AAS is the system that the Commission uses to facilitate the sale of unused spectrum to the public and includes a web-based component utilized by bidders to register for auctions and place bids.

Factors including the high visibility of the auction process, criticality of functions and significant financial investment in the automated systems warranted the determination for an audit of the AAS application security and controls. The audit was performed with the intent of identifying weaknesses that could result in external and internal exploits.

The Office of Inspector General (OIG) engaged KPMG LLP to perform an audit of the AAS. The objective of this audit was to determine the extent and effectiveness of application controls for the AAS. To achieve our objectives, we performed a Federal Information Systems Control Manual (FISCAM) based application and general controls review of the AAS, including its web-based component. A review of technical controls was conducted on the AAS database to identify internal and external vulnerabilities that may lead to compromise of the database. For the application control piece, we evaluated authorization controls, completeness controls, accuracy controls, and controls over integrity of processing and data files. For the general controls review, we evaluated the major categories of general controls such as: the risk assessment process, access controls, system software, service continuity, security program planning and management, and application change controls. Our review of technical controls consisted of scans of specific internal network segments on the Auction network and limited scans of the external network.

Our review yielded several positive security observations. They are noted as follows:

1. Security plans for the Automated Auction System (AAS) and the Auctions network, that incorporate elements recommended by OMB-130 for major applications, have been developed and implemented.
2. There appears to be adequate segregation of duties for AAS administration, programming, and testing.
3. Controls related to the completeness, authorization and accuracy of data during the Auction Definition stage appear adequate.

During the audit, we also identified areas of improvement for the Wireless Telecommunication Bureau's (WTB) security controls over the AAS. This report details the conditions identified during our audit and communicates findings and recommendations to FCC management. Specifically, we identified fourteen (14) findings in the areas of management, operational, and technical controls. Of the fourteen findings, one (1) is rated as high risk, ten (10) as medium risk, two (2) as low risk and one (1) finding with both high-risk and medium-risk components. We recommend that the recommendations for those deficiencies identified be fully implemented to strengthen the security of the AAS application and data. Our recommendations are intended to correct present vulnerabilities and should effectively minimize the risk of occurrence of future security-related events.

On April 11, 2002, we presented preliminary findings to WTB and the Information Technology Center (ITC) at the key milestone meeting to obtain clarification of the facts of conditions identified. In response, WTB provided informal written comments on April 16, 2002 and again on April 29, 2002. Additionally, follow-up meetings were conducted on April 18, 2002 and May 9, 2002 to ensure WTB's agreement on the facts of the findings that are presented in this report. We modified the conditions as necessary to reflect informal written comments provided by WTB and reached agreement with WTB on the facts of the findings noted.

On June 6, 2002, we issued a draft report summarizing the results of our audit. In that draft report, we requested that WTB respond to the findings and recommendations presented in our report. WTB provided responses to the fourteen (14) findings.

In a response dated June 21, 2002, WTB indicated concurrence with the recommendations made for all fourteen findings. For all findings, WTB outlined the corrective action taken and/or a milestone schedule for implementation of corrective action. WTB did not concur with the two "High" risk levels for Findings TC-01 and TC-02. We have included a copy of the response from WTB in its entirety as Appendix C to this report. Where WTC disagreed with the risk levels, we have added a section titled "OIG Comments," to explain our position.

Because of the sensitive nature of the information contained in the appendices, we have marked them all "Non-Public – For Internal Use Only" and have limited distribution. Those persons receiving this report are requested not to photocopy or otherwise distribute this material.

Background

Factors including the high visibility of the auction process, criticality of functions and significant financial investment in the automated systems warranted OIG's determination for an audit of the AAS application security and controls. It is imperative that the AAS be secured against external threats as well as internal threats. The audit, specifically the review of technical controls, was conducted to identify vulnerabilities that could result in external and internal exploitation of the database.

Much attention is given to system and network attacks resulting from external attacks upon a network, which are easier to detect, and much more publicized. However, equally important is the threat of internal attacks by users who have some degree of authorization on the network. In a recent article published on April 12, 2002 by Computerworld entitled, "Insider Threat to Security May Be Harder to Detect, Experts Say", leading industry experts from the Federal Bureau of Investigations' National Infrastructure Protection Center and the Federation of American Scientists addressed the reality of internal security threats. The article reported that the most devastating threats to computer security have come from individuals who are deemed trusted insiders within the organization. The article also reported that the most effective insiders are often "keyholders" who have access to internal systems based on contracts or partnerships with an organization. Such internal attacks are more difficult to detect. With increasing reliance of the FCC on contracted agreements and the revolving nature of contract staffing, such threats exist at the Commission.

The guideline for performing this audit was the Federal Information System Control Audit Manual (FISCAM). Additional guidance was received from National Institute of Standards and Technology (NIST) and Federal Information Processing Standards (FIPS) publications, as well as the following laws and directives related to management and protection of Federal information resources:

- Presidential Decision Directive (PDD) 63 entitled "Critical Infrastructure Protection".
- PDD-67, entitled "Continuity of Operations Planning (COOP)".
- Office of Management and Budget (OMB) Circular A-130 entitled "Management of Federal Information Resources", as revised on November 30, 2000.
- OMB 97-16 entitled "Information Technology Architectures".
- OMB 98-02 entitled "Funding Information Systems Investments".
- The Computer Security Act of 1987 (PPL 100-235).
- FCC Instruction 1479.1 and 1479.2, "Computer Security Program Directive".

Objective

The purpose of this audit was to examine the AAS application and the information technology (IT) infrastructure supporting the application to ensure that systems are adequately secured consistent with Federal regulations governing the management of critical information systems. The scope of the audit included the security infrastructure managed by the Office of Managing Director's Information Technology Center (ITC) and the Auctions Automation Branch of the WTB.

The specific objectives of the evaluation were to:

- Obtain an understanding of the Commission's AAS application infrastructure, including its security and controls.

- Obtain an understanding of the Commission's information security program and practices;

- Use application assessment methodologies, such as the Federal Information Systems Control Manual (FISCAM), to evaluate the effectiveness of the information security and controls of the AAS. The evaluation included a review of the database technical controls to determine its vulnerability to internal and external exploits.

- Prepare a detailed report that (1) identifies the critical AAS security control deficiencies, if any, and (2) contains observations and recommendations for improvement, if any.

An application controls review of the AAS application was performed to examine the accuracy, completeness and authorization of input/output controls over the AAS application and processes. A general controls review of the AAS application was performed to examine security controls related to the risk assessment process, access controls, system software, service continuity, security program planning and management, and application change controls. The findings related to operational and management controls were identified during the application and general controls reviews.

A review of technical controls was conducted on the AAS database to identify internal and external vulnerabilities that may lead to compromise of the database. We assessed the AAS database security posture by performing audit steps from the following four user perspectives:

- An outsider without knowledge about FCC Auctions IT environment attempting to access the Database Server from the public Internet.
- A typical user on the FCC Local Area Network (LAN).
- A typical applications user, with low-level privileges to the Auctions database.
- A high level Database Administrator (DBA), with full access to the Auctions database.

While on the internal network, we performed technical controls testing that included port scanning, user enumeration, vulnerability scanning, and performance of other techniques to detect possible exploitable weaknesses. The external assessment consisted of limited, high-level scanning of the network. All findings related to deficiencies in technical controls were identified during our review of technical controls.

Scope

The scope of this review included the security infrastructure managed by the Office of Managing Director's Information Technology Center (ITC) and the Auctions Automation Branch of the WTB. Our approach consisted of reviewing documentation that included previous special reviews and audits, conducting interviews, attending meetings, conducting a technical controls review and from observations.

Our procedures were designed to comply with applicable auditing standards and guidelines. These included the American Institute of Certified Public Accountants' (AICPA) Professional Standards, Generally Accepted Government Auditing Standards (GAGAS) as well as GAO's Federal Information Systems Control Audit Methodology

(FISCAM). We also used other professionally recognized and accepted authorities as necessary. Our methodology for the technical controls review was developed to identify the more well-known and exploited information systems vulnerabilities to determine if they exist within the Auctions' information technology environment.

The observations from our review are organized according to areas of management controls, operational controls, and technical controls. Within each control area, specific control objectives are addressed.

Management Controls - Management controls focus on the management of the IT security system and the management of risk for a system. They are techniques and concerns that are normally addressed by management. The specific management control objectives addressed are:

- Risk Management
- System Security Plan

Operational Controls - The operational controls address security methods focusing on mechanisms primarily implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise and often rely upon management activities as well as technical controls. The specific operational control objectives addressed are:

- Production, Input/Output Controls (including accuracy, completeness and authorization controls)
- Access Controls
- Service Continuity
- System Software
- Change Control

Technical Controls - Technical controls focus on security controls that the computer system executes. The controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. The specific technical control objectives addressed are:

- Identification and Authentication
- Audit Trails
- Logical Access Controls

Each finding has been further categorized by risk ratings of 'High', 'Medium' or 'Low'. In assigning ratings, we considered whether each condition, if exploited, could result in misuse or loss of the AAS application and its data, as well as the potential degree of exposure to FCC. Additionally, we considered the potential level of business disruption to the Commission if the reported conditions were exploited. Some examples of business disruptions include system downtime, lost productivity related to staff time shifted away from normal business operations to address security-related issues and the effects of security events on customer confidence. The risk ratings are defined below:

High Risk: A security risk which can cause a business disruption, if exploited. The identified condition presents a level of risk that requires immediate and appropriate redress by WTB management. Failure to address this condition would have the potential effect of increasing the risks of unnecessary system downtime, misuse and destruction/exposure of critical FCC data.

Medium Risk: A security risk that, in conjunction with other events, can cause a business disruption, if exploited. It is important for WTB management to take appropriate corrective action on these medium-risk security control conditions in order to protect the integrity, availability, and confidentiality of FCC data.

Low Risk: Security risk may cause operational annoyances, if exploited.

Observations

Our review yielded several positive security observations as well as deficiencies that require corrective actions. Positive security observations include the following:

1. Security plans for the Automated Auction System (AAS) and the Auctions network that incorporates elements recommended by OMB-130 for major applications has been developed and implemented.
2. There appears to be adequate segregation of duties for AAS administration, programming, and testing.
3. Controls related to the completeness, authorization and accuracy of data during the Auction Definition stage appear adequate.

Although the Commission has implemented numerous positive controls over the AAS, we identified fourteen (14) findings that impact the effectiveness of security and control of the application. Prior to issuance of this report, the WTB began to proactively take steps to address these findings. We recommend that the recommendations for those deficiencies identified be fully implemented to strengthen the security of the AAS application and data. Our recommendations and those actions already begun by WTB management should result in the correction of present vulnerabilities and minimization of the risk of occurrence of future security-related events.

Appendix A of the report, entitled Summary of Findings, provides a summary of the findings from this review; Appendix B, entitled Detailed Findings and Recommendations, provides detailed information on the conditions identified, criteria used to evaluate the condition, effect, and recommendation(s). Appendix C, entitled WTB Response, provides WTB's reply to this audit.

In accordance with the Commission's directive on the management of non-public information, we have classified all appendices as "Non-Public – For Internal Use Only." Those persons receiving this report are expected to follow the established policies and procedures for managing and safeguarding this report in accordance with the Commission directive.