Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

PENETRATION TEST OF THE INDIAN HEALTH SERVICE'S COMPUTER NETWORK

Inquiries about this report may be addressed to the Office of Public Affairs at Public.Affairs@oig.hhs.gov.

Thomas M. Salmon
Assistant Inspector General

March 2014
A-18-13-30330

Office of Inspector General

https://oig.hhs.gov

The mission of the Office of Inspector General (OIG), as mandated by Public Law 95-452, as amended, is to protect the integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of beneficiaries served by those programs. This statutory mission is carried out through a nationwide network of audits, investigations, and inspections conducted by the following operating components:

Office of Audit Services

The Office of Audit Services (OAS) provides auditing services for HHS, either by conducting audits with its own audit resources or by overseeing audit work done by others. Audits examine the performance of HHS programs and/or its grantees and contractors in carrying out their respective responsibilities and are intended to provide independent assessments of HHS programs and operations. These assessments help reduce waste, abuse, and mismanagement and promote economy and efficiency throughout HHS.

Office of Evaluation and Inspections

The Office of Evaluation and Inspections (OEI) conducts national evaluations to provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. These evaluations focus on preventing fraud, waste, or abuse and promoting economy, efficiency, and effectiveness of departmental programs. To promote impact, OEI reports also present practical recommendations for improving program operations.

Office of Investigations

The Office of Investigations (OI) conducts criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs, operations, and beneficiaries. With investigators working in all 50 States and the District of Columbia, OI utilizes its resources by actively coordinating with the Department of Justice and other Federal, State, and local law enforcement authorities. The investigative efforts of OI often lead to criminal convictions, administrative sanctions, and/or civil monetary penalties.

Office of Counsel to the Inspector General

The Office of Counsel to the Inspector General (OCIG) provides general legal services to OIG, rendering advice and opinions on HHS programs and operations and providing all legal support for OIG's internal operations. OCIG represents OIG in all civil and administrative fraud and abuse cases involving HHS programs, including False Claims Act, program exclusion, and civil monetary penalty cases. In connection with these cases, OCIG also negotiates and monitors corporate integrity agreements. OCIG renders advisory opinions, issues compliance program guidance, publishes fraud alerts, and provides other guidance to the health care industry concerning the anti-kickback statute and other OIG enforcement authorities.

Notices

THIS REPORT IS AVAILABLE TO THE PUBLIC
at http://oig.hhs.gov

Section 8L of the Inspector General Act, 5 U.S.C. App., requires that OIG post its publicly available reports on the OIG Web site.

OFFICE OF AUDIT SERVICES FINDINGS AND OPINIONS

The designation of financial or management practices as questionable, a recommendation for the disallowance of costs incurred or claimed, and any other conclusions and recommendations in this report represent the findings and opinions of OAS. Authorized officials of the HHS operating divisions will make final determination on these matters.

The Indian Health Service needs to address cyber vulnerabilities on its computer network.

This report provides an overview of the results of our penetration test of the Indian Health Service's (IHS) computer network. It does not include specific details of the vulnerabilities that we identified due to the sensitive nature of the information. We have provided more detailed information and recommendations to IHS so that it can address the issues we identified.

WHY WE DID THIS REVIEW

Computer hackers are increasingly attempting to compromise Government systems, publish sensitive data, and use stolen data to commit fraud. Threats to Federal agency Web applications are continually changing because of advances made by hackers, the release of new technology, and the deployment of increasingly complex systems. Web sites that are not secured properly create vulnerabilities that could be exploited by an unauthorized user to compromise the confidentiality of sensitive information. Furthermore, cyber attacks through targeted email messages constitute the vast majority of attacks on Federal and private sector networks, according to Federal data. These attacks could significantly impact the operations of Federal agencies and expose sensitive data.

Previously, in 2011, we conducted a separate information technology (IT) general controls audit of the IHS's network security controls and found that such controls were inadequate. The security vulnerabilities identified presented an increased risk that unauthorized individuals could gain access to the IHS network and potentially to the U.S. Department of Health and Human Services (HHS) network. Therefore, in June 2013, we decided to conduct further testing of the effectiveness of IHS's network security controls by performing an external network penetration test. The objective of this review was to determine whether IHS network systems were susceptible to compromise by cyber attacks.

BACKGROUND

Penetration tests are used to identify methods of gaining access to a system by using tools and techniques that attackers use. This audit was the first of a series of OIG audits planned to include penetration testing of HHS and its operating division's networks.

IHS, which is 1 of 12 HHS operating divisions, provides health services directly through tribally contracted and operated health programs and through services purchased from private providers. The Federal system consists of 28 hospitals, 61 health centers, and 34 health stations. In addition, 33 urban Indian health projects provide a variety of health and referral services. Protecting beneficiaries' and providers' personally identifiable information and personal health information is critical because fraud perpetrators often use stolen beneficiary or physician identities, or both, to submit false claims to the programs.

HOW WE CONDUCTED THIS REVIEW

We assessed the IHS network's exposure to cyber attacks by performing a penetration test of its networks and information systems. We conducted the penetration test from June 10 through 14, 2013, with the knowledge and permission of IHS officials. We requested that IHS incident response staff not be notified of our testing to assess the effectiveness of IHS's intrusion detection and response controls. Appendix A contains a summary of our audit scope and methodology.

Risk Level Definitions for Findings

To assign risk levels (i.e., High, Medium, Low) to our findings, we used Table 3-7, "Risk Scale and Necessary Actions," of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, *Risk Management Guide for Information Technology Systems*, which describes the need for corrective actions and the relative timeframes in which they must occur based on high, medium, and low levels of risk associated with system vulnerabilities. Appendix B contains the table.

WHAT WE FOUND

Overall, the IHS needs to address cyber vulnerabilities on its computer network. Specifically, we were able to obtain unauthorized access to an IHS Web server and an IHS computer.

- We were able to gain unauthorized access to an IHS Web server, which allowed us to access the internal IHS network and obtain user account and password data on the system, including user names and passwords to IHS databases (High Risk).

- We were able to take control of an IHS computer, which allowed access to the computer's resources, including records in the file system (Medium Risk).

Due to the sensitive nature of the specific findings identified during our testing, only a summary of the findings are included in this report. We have provided more detailed, technical findings to IHS.

WHAT WE RECOMMEND

We made 6 recommendations to IHS to address the security vulnerabilities that we identified. In general, we recommended that IHS fix the vulnerability on the IHS Web server, implement more effective procedures to protect its computer systems from cyber attacks, and periodically measure adherence to IHS security policies and procedures.

This report summarizes our recommendations due to the sensitive nature of the information discussed. We have provided more detailed recommendations to IHS.

AUDITEE COMMENTS

In written comments to our draft report, IHS concurred with all of our recommendations and described the actions they will take to implement them.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

We focused our audit on the IHS network and Web sites in operation during the period June 10 through 14, 2013. We did not review IHS's overall internal control structure. We performed our testing from OIG facilities.

METHODOLOGY

To accomplish our objectives, we prepared a Rules of Engagement document that outlined the general rules, logistics, and expectations for the penetration test and obtained signatures from both IHS and OIG management. Afterwards, we performed the following procedures:

- conducted information-gathering techniques to discover the following for IHS:
    - network address ranges,
    - host[5] names,
    - exposed hosts,
    - applications running on exposed hosts,
    - operating system and application version information,
    - current patch levels of the hosts and applications,
    - structure of the applications and supporting servers, and
    - domain name server records;
- conducted vulnerability analysis techniques to discover possible methods of attack;
- exploited vulnerabilities identified in the vulnerability analysis to attempt to gain root or administrator-level access to the target systems or other trusted user account access;
- used advanced techniques to gain access to an IHS computer system and attempted to gain a persistent foothold into the network and to escalate user privileges; and
- discussed our findings with IHS management.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[5] A host is any device connected to a computer network.

APPENDIX B: RISK SCALE AND NECESSARY ACTIONS

Risk Level	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, the system's designated approving authority must determine whether corrective actions are still required or decide to accept the risk.