



Homeland
Security

May 22, 2007

Clifford Jennings
Inspector General
Appalachian Regional Commission
1666 Connecticut Avenue, NW
Washington, DC 20009

SUBJECT: Evaluation of the Appalachian Regional Commission's Systems Security Program

At your request we conducted an information security evaluation of the Appalachian Regional Commission's (ARC) information systems and operations. Our objective was to determine whether the logical access controls and the systems security environment were adequate to protect the commission's sensitive data. We provided the ARC with the results of our vulnerability scans, and are providing our specific findings in this letter.

ARC has not fully implemented effective information security policies, procedures, or practices. Most significant is that access controls, such as user account rights and permissions, are not applied for the databases that contain the agency's data, nor the systems used to connect to the databases. Core security practices such as separation of duties, configuration management, and disaster recovery are also not implemented. As a result, sensitive data at ARC are at risk to unauthorized access, use, disclosure, or destruction. These risks from internal and external threats could jeopardize the integrity of financial documents stored on the systems. ARC is in the process of building a systems security program to protect the integrity of its data and systems. Risks to mission-critical data will remain until this program is fully developed, documented, and implemented.

Background

The ARC is a federal state partnership that works with the people of Appalachia to create opportunities for self-sustaining economic development and improved quality of life. Each year ARC provides funding for several hundred projects throughout the Appalachian Region, in support of its goals to:

- Increase job opportunities;
- Strengthen the capacity of people to compete in the global economy;
- Develop and improve infrastructure; and
- Reduce isolation through the Appalachian Development Highway System.

These projects create thousands of new jobs, improve local water and sewer systems, increase school readiness, expand access to health care, assist local communities with strategic planning, and provide technical, managerial, and marketing assistance to emerging new businesses.

The information systems environment at ARC is designed to provide local and remote business services to its users. This environment is composed of approximately 60 workstations and 12 servers that run office support applications, and provide web content and database management software. In addition, ARC supports a wide variety of mobile users through its virtual private network capability.

Although ARC is not governed by agency-specific regulations, best practices for information security in the federal government apply, and can be found in legislation such as the *Federal Information Security Management Act of 2002*, the *E-Government Act of 2002*, and the *Office of Management and Budget Circular A-130, Management of Federal Information Resources*. References for detailed, system best practices can be found in special publications from the National Institute of Standards and Technology.

We conducted this evaluation through interviews with ARC staff using software tools to perform network and system vulnerability tests and by direct observations of the evaluation team. We used Tenable Nessus, Retina, and Application Security's AppDetective to perform our vulnerability testing. We conducted our evaluation from August to September 2006 under the authority of the *Inspector General Act of 1978*, as amended, and according to the *Quality Standards for Inspections* issued by the President's Council on Integrity and Efficiency.

Access Controls Provide Foundation for Strong Security

Access control measures such as minimum password length requirements, automatic session timeouts, file level permissions, and security event logging were not implemented at ARC. Employing such measures provide a defense in depth approach to information systems security.

Users logging on to ARC systems were required to enter a password. However, users could select passwords of any length, those easily guessed or common dictionary words, and those able to be reused multiple times upon reset. Further, our scan results showed that passwords for access to the ARC network were set to never expire. Despite those results, some users report having been required to change their passwords periodically. As a security precaution, setting a minimum length for all passwords for user accounts provides a first line of defense against unauthorized access. The longer the password, the more difficult it is to be discovered by trial and error. Password security also can be strengthened through the use of password expiration times. Passwords should be set to expire, as a protection against compromise and unauthorized use.

The configuration of ARC systems allowed users, once logged on, to remain connected for an indefinite period of time, despite periods of inactivity. System administrators can use session timeouts to ensure that users are disconnected from network resources after a period of inactivity, to prevent unattended systems from unauthorized use. Setting an automatic timeout to 20 minutes, for example, would add another layer of access control and security to the ARC network.

All user folders stored on ARC's network were accessible to anyone authorized on the system from any workstation. As a result, all data on the network were available for viewing, copying, or deletion by any and all employees. The purpose of file servers at ARC is to provide for the transfer and storage of files for authorized users. Malicious users can take advantage of incorrectly

configured file servers to read, copy, alter, or delete, material without the knowledge or permission of the owner.

Security event logging was disabled on all systems limiting management's ability to respond to incidents or suspicious activity. Security event logging is the automated documenting of all security events for an application or a system. Event elements such as user, workstation, login and logout, applications or web pages accessed, documents changed or deleted, and attempted failed logins should be recorded. These elements are captured in order to maintain a timeline of events. These logs can be reviewed by security personnel or management to recreate incidents and trace the specific origin of potential attacks on resources, data, or equipment.

Unchallenged Virtual Private Network Access Presents Risks

Remote connections are allowed to its network from any computer, including those not owned and maintained by ARC. By allowing these connections, ARC resources and data are at significant risk for possible infection by viruses and malware potentially resident on home computers or other non government-owned devices. Common best practice among federal agencies is to deny access to any system not owned, operated, and maintained by the agency's information technology support team.

In addition, virtual private network (VPN) connections were not monitored or logged for security events. This condition allows for any potentially unprotected home computer to have full access to the data and devices at ARC, without any record for investigation should an intrusion occur. Unusual or unauthorized events can be detected through the review of log data, assuming that the correct data is being logged and reviewed. The definition of what constitutes unusual activity varies, but can include failed login attempts, login attempts outside of designated schedules, locked accounts, port sweeps, network activity levels, and memory utilization.

Systems Security Management Remains Vital to Program Success

The majority of users at ARC have "administrative privileges" on their workstations, thereby granting rights beyond what is required for them to perform their job responsibilities. For example, all users were granted default access to one of ARC's databases, allowing users to move, change, or delete data without the authority to do so. These privileges allow for configuration changes, unauthorized software installations, and disabling of integrated security features and as a result, increase risk to system and network security. Administrative privileges can further be used to gain access to resources that normally would be protected from an application or user such as the ability to delete critical system files. User rights should be granted using the least privilege principle. Under the least privilege principle, a process, a user, or a program must be able to access only such information and resources that are necessary for its legitimate purpose.

No configuration guide was used for the installation of workstation, server, and database software. This software should be configured and maintained using the built-in security features of the manufacturer to protect data. Baseline software security installation guides are available to assist network administrators in applying security measures within specific operating systems and applications. These guides provide settings, configurations, and methods to protect the data under their control.

The patch management program is ineffective, as was evident with the failure of the deployment of a critical patch, the recent “daylight savings time” update. Microsoft Windows servers were found to be missing critical security updates, including those containing ARC’s public-facing web services. The Microsoft SQL database, ARC’s main repository of its financial data, is missing 29 critical security patches dating back to 2004. The Windows Server software hosting this application has not been patched since 2001. Overall, a total of 603 security vulnerabilities were found on the systems at ARC, with 153 identified as high risk, 265 as medium risk, and 185 as low risk. To combat constantly evolving attack methods, system software should be periodically updated to provide the most protection currently available.

In addition, several other administration weaknesses further detract from ARC system security:

- ARC uses server software, such as Microsoft Windows NT Server, which is no longer supported by the manufacturer and has not been since 2004. Outdated and unsupported software no longer receives security updates and can be exploited.
- All network administration duties at ARC were performed by the same position. This arrangement does not provide for adequate technical oversight of systems security. Separation of system administrator duties is one of the key concepts of internal control.
- The backup and disaster recovery practices are minimal, and no offsite backups of critical data were found. Although ARC has employed a remote backup solution to protect its critical data from disaster, procedures to restore that data were not documented.
- No formal information security training is being conducted for users on the ARC network.
- Housekeeping issues, poor network cable management, and ceiling water damage were observed in the commission’s server room.

Misuse of Government Equipment Emphasizes the Need for Controls

In the course of our evaluation, a single folder containing approximately 400 gigabytes of inappropriate material was found on the ARC network. Peer-to-peer file sharing software, designed to provide access to local resources, was found on a workstation operated by the owner of the folder. This folder and its contents represent the misuse of government equipment to store material that could be copyrighted or pornographic in nature, as well as the potential to distribute the material in a manner rendering the system vulnerable. Without system logs, it was not possible to document the volume of files distributed nor the impact on system resources over and above the storage space required.

When brought to the attention of ARC senior management and in consultation with the ARC Inspector General, immediate action was taken to correct this activity. Additional measures were put in place to protect ARC assets, including the disabling of the VPN and changing of all system passwords.

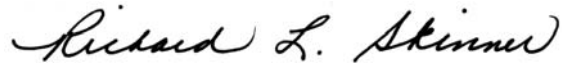
Recommendations

We recommend that the Executive Director, Appalachian Regional Commission:

- **Recommendation #1:** Ensure that security policy based on National Institute of Standards and Technology guidance is issued and that users are trained on system security principles and practices.
- **Recommendation #2:** Ensure that security controls are implemented to include password restrictions, session timeouts, file-level permissions, and security log controls.
- **Recommendation #3:** Ensure that VPN access is controlled through the use of agency-issued equipment only.
- **Recommendation #4:** Ensure that an Information Systems Security Officer position is established with a defined role and assigned responsibilities for the implementation of the commission's systems security plan.

Should you have any questions, please call me, or your staff may contact Frank Deffer, Assistant Inspector General, Information Technology, at (202) 254-4100.

Sincerely,



Richard L. Skinner
Inspector General