WRITTEN STATEMENT OF

WILLIAM R. MCCOLLUM, JR.
Chief Operating Officer

Tennessee Valley Authority

Before the

HOUSE COMMITTEE ON HOMELAND SECURITY SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY

"Implications of Cyber Vulnerabilities on the Resiliency and Security of the Electric Grid"

May 21, 2008

William R. McCollum, Jr.
Chief Operating Officer
Tennessee Valley Authority

Good afternoon Chairman Langevin, Ranking Member McCaul, and members of the Subcommittee. I am Bill McCollum, Chief Operating Officer of the Tennessee Valley Authority (TVA). I am accompanied today by TVA's Chief Administrative Officer, John Long.

I appreciate this opportunity to appear before you to discuss the Government Accountability Office (GAO) report on the security of the computer networks and control systems used in TVA's operations.

As TVA's Chief Operating Officer, I am responsible for the safe and reliable operation of the TVA power system, which generates and distributes electricity for a region of the Southeast which covers Tennessee and adjacent parts of six neighboring states. All of our operations –the generation and distribution of electricity and our stewardship of the Nation's fifth largest river system and economic development work – are financed by revenue from the sale of electricity. TVA does not receive any annual congressional appropriations.

I am pleased to note that earlier this week we observed the 75th Anniversary of TVA in Muscle Shoals, Alabama. As we have for 75 years, we remain focused carrying out our historic three-part mission in energy, economic development and environmental stewardship. Each part of our mission has contributed significantly to the progress of our 80,000-square-mile service region, which is centered on the watershed of the Tennessee River.

In performing our mission, the safety of our employees and the public is paramount in all of our operations, including the specialized security requirements to protect the computerized control systems involved in the generation and transmission of electricity.

On behalf of TVA, we appreciate the substantial time and resources that the GAO allotted to examining and evaluating our computer security. As you know, the report made public today by the GAO listed 19 recommendations for improving the security of our computer systems. We concur with all of those recommendations, and we have either completed or are aggressively moving to implement remedial actions for all 19.

It is important to note that TVA was already in the process of addressing 17 of the 19 recommendation areas when GAO's field work began at TVA last October. We also initiated several actions to address other aspects of our security while the field team was conducting its evaluation. These actions were the result of on-going assessments by TVA staff and the independent TVA Office of Inspector General, which had initiated planning for an audit of our Information Technology Security by Science Applications International Corporation. GAO's work has been very helpful in affirming and focusing the need for these and other measures that we are taking.

Some of the security issues identified by the GAO report involved instances that have been addressed by the centralization of our cyber security policy, its administration and its oversight activities into a corporate-level organization. The centralization of this responsibility was completed in February, which now gives TVA uniform security procedures to be followed by all of its organizations and covers all control systems.

In conjunction with our implementation of additional measures to strengthen our defense-in-depth security posture, we commissioned a third-party consultant to perform penetration testing of our infrastructure to identify any immediate weaknesses. The testing involved both "informed" and "uninformed" circumstances in which this third party made attempts to penetrate our networks. We are pleased to note that the consultant's team was unable to gain access to any of the targeted Process Control Networks in either type of test. While the tests failed to penetrate our control network security, the process identified several opportunities to further insulate and protect the security of our systems. We are now implementing those additional measures.

In closing, TVA fully understands that it has a solemn responsibility to ensure the safety and security of systems that are vital to the nation's critical infrastructure, our region and nation's economy, and the health and safety of the public. As the Chief Operating Officer, one of my responsibilities is ensuring that we embrace safety as a value in all aspects of our operations to protect the health and well-being of our workforce and the public. We are moving as quickly as possible to complete remedial measures for all 19 of GAO's recommendations, along with other steps we have identified, to elevate every level of our computer and network security.

As a federal entity, we are cognizant of our special responsibility to provide leadership in this important aspect of electric system operations. We assure the Subcommittee and the public at-large that TVA is committed to assuring that the infrastructure entrusted to our responsibility meets or exceeds the best accepted practices in government and in the electric utility industry.

Thank you for this opportunity to provide our perspectives and experiences as you continue the Subcommittee's important work in assessing the adequacy of security measures within the Nation's critical electric power infrastructure.

# # #