U.S. Environmental Protection Agency
Office of Inspector General

2005-P-00002
January 6, 2005

At a Glance

Catalyst for Improving the Environment

Why We Did This Review

Federal Directives highlighted the need to secure cyberspace, including SCADA, from terrorists and other malicious actors, and stated that securing SCADA is a national priority. We learned from stakeholder contacts that utilities may require assistance in order to secure their SCADA system vulnerabilities.

Background

SCADA is a technology that allows a user to collect data from sensors and control equipment, such as pumps and valves, from a remote location. SCADA is commonly used in many industries, including water utility operations.

We suspended our SCADA project because EPA agreed to incorporate our concerns into an Agency SCADA project. At EPA's request, we briefed the Agency on our preliminary research and prepared this briefing report.

For further information, contact our Office of Congressional and Public Liaison at (202) 566-2391.

To view the full report, click on the following link:

www.epa.gov/oig/reports/2005/20050106-2005-P-00002.pdf

EPA Needs to Determine What Barriers Prevent Water Systems from Securing Known Supervisory Control and Data Acquisition (SCADA) Vulnerabilities

What We Found

SCADA networks were developed with little attention paid to security. As a result, many SCADA networks may be susceptible to attacks and misuses. Furthermore, studies indicated that some water utilities may have spent little time and money securing their SCADA systems.

Some areas and examples of possible SCADA vulnerabilities include operator errors and corruption, unsecured electronic communications, hardware and software limitations, physical security weaknesses, natural disasters, poorly written software, and poor security administration. Vulnerabilities may allow a person of malicious intent to cause significant harm. For example, in 2000, an engineer used radio telemetry to gain unauthorized access into an Australian waste management system and dump raw sewage into public areas. In another example, a contractor conducting a utility water assessment stated that he was able to access the utility's network from a remote location within minutes and could have caused significant harm.

Through preliminary research, we found several possible reasons why utilities have not successfully reduced or mitigated identified vulnerabilities. It is important to note that this list is not in any way expected to be exhaustive of what a full study may reveal. Specifically:

- Current technological limitations may impede implementing security measures.
- Companies may not be able to afford or justify the required investment.
- Utilities may not be able to conduct background checks on existing employees.
- Officials may not permit SCADA penetration testing.
- Technical engineers may have difficulty communicating security needs to management.

To better enable water systems to secure their SCADA systems, we suggest that EPA identify impediments preventing water systems from successfully reducing or mitigating SCADA vulnerabilities, and take steps to reduce those impediments. If EPA identifies a problem with no apparent solution, the Agency should communicate this problem to the Department of Homeland Security, Congress, and others as appropriate. We also suggest that EPA develop SCADA security measures to track the effectiveness of security efforts.