



One Hundred Tenth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

February 9, 2007

The Honorable David M. Walker
Comptroller General of the United States
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. Walker:

Control systems, the computer-based systems that monitor and control sensitive processes and physical functions, support the operation of a significant part of the nation's critical infrastructure. As your previous work has shown, these systems are vulnerable to cyber and physical attacks that could result in loss of service, physical damage, loss of life, and severe economic impact. These systems have already been subject to numerous cyber attacks, and securing them poses significant challenges. The Department of Homeland Security ("Department") has established the Control Systems Security Program to guide government and industry efforts to improve the security of control systems within the nation's critical infrastructure.

We would like GAO to update the committee on the cybersecurity risks associated with these control systems, evaluate the Department's efforts to secure controls systems, and identify the challenges the Department faces in securing control systems.

For further questions about this request, please contact Jacob Olcott or Cherri Branson at (202) 226-2616.

Sincerely,

Handwritten signature of James R. Langevin in black ink.

James R. Langevin
Chairman
Subcommittee on Emerging Threats,
Cybersecurity, and Science
and Technology

Handwritten signature of Michael T. McCaul in black ink.

Michael T. McCaul
Ranking Member
Subcommittee on Emerging Threats,
Cybersecurity, and Science
and Technology

February 8, 2007

Page 2



Sheila Jackson-Lee
Chairwoman
Subcommittee on Transportation
Security and Infrastructure Protection



Daniel E. Lungren
Ranking Member
Subcommittee on Transportation
Security and Infrastructure Protection