

Statement of James F. McDonnell  
Director, Protective Security Division,  
Information Analysis and Infrastructure Protection Directorate  
Department of Homeland Security  
Before the  
Government Reform Committee's Subcommittee on Technology, Information Policy,  
Intergovernmental Relations and the Census  
U.S. House of Representatives  
March 30, 2004

Good morning Chairman Putnam and distinguished Members of the Subcommittee. It is an honor to appear before you today to discuss activities that the Department of Homeland Security is engaged in regarding process control systems in our Nation's critical infrastructure. I am James McDonnell, Director of the Protective Security Division (PSD), part of the Department's Information Analysis and Infrastructure Protection Directorate (IAIP).

Established by the *Homeland Security Act*, and directed by Homeland Security Presidential Directives, IAIP is responsible for reducing the Nation's vulnerability to terrorism by:

- Developing and coordinating plans to protect critical infrastructure and key assets.
- Denying the use of our infrastructure as a weapon.

Our goal is to ensure a national capacity to detect indicators of terrorist activity, deter attacks, and devalue targets and to defend potential targets against terrorist threats to our critical infrastructure.

To meet this goal, IAIP identifies those sites and facilities that may be attractive targets for terrorists based on risk and identifies how target vulnerabilities may be exploited by terrorists. Once we know what we should protect and what the vulnerabilities are, we conduct risk assessments, mapping threat and vulnerability information. This information is then used to prioritize the implementation of protective measures focused on mitigating our Nation's vulnerability to attack and, more importantly, shared in a timely manner with State and local officials.

Terrorist acts come in many forms. Some result in loss of life, others in severe economic consequences. Some, like September 11, result in both. Terrorist attacks do not have to follow a pattern and may range from a bombing by an individual to a global internet-based cyber attack. Protecting our way of life means understanding the myriad of vulnerabilities and the associated interdependencies and cascading effects.

The complexity of the infrastructure requires a comprehensive understanding of how the “system of systems” operates and it is this complexity that adds another dimension of vulnerability: the use of complex process control systems.

Process control systems (PCS) are industrial measurement and control systems used to monitor and control plants or equipment. They are utilized in numerous industries, including energy, manufacturing, chemical production and storage, food processing, and drinking water and water treatment systems. PCS are often referred to generically by one of the most prevalent types, SCADA, or Supervisory Control and Data Acquisition, but there are other types such as Distributed Control Systems (DCS).

These systems vary in function, size, complexity, and age. Some function in an automated fashion. Some rely on a human/machine interface, where the system provides critical information upon which an operator bases process control decisions. Some digital control systems can be “reprogrammed” from off-site through dial-up connections or through web-based access. This physical-cyber nexus creates a complexity which requires a comprehensive approach for protection.

Some methodologies for cyber and physical vulnerability assessments have not taken into account the implications of a process control systems failure on the operation or safety of the infrastructure. In addition, exclusively cyber, personnel, or physical security measures leave process control systems open and accessible. Protective measures must be responsive to all aspects of vulnerabilities regardless of the path for delivery and must keep pace with changes in technology.

SCADA systems were originally designed to be an isolated operational system with no outside path to access the system. However, competitive, economic, and technological pressures have opened these systems to corporate and vendor networks. Some SCADA networks have been joined to business networks with no air-gap technology emplaced and vendor networks have 24x7 accesses to critical SCADA systems for maintenance purposes. Moreover, both operating plant and SCADA staff use remote terminals for after-hour’s maintenance via LAN or dial-up connections, leaving themselves open to cyber attacks. In most cases, remote terminal units can be accessed by anyone with a modem dialer. More often than not, systems will have no passwords, default passwords, or passwords as simple as “1234”. Passwords are routinely left at the “out-of-the-box” default and rarely changed for fear of affecting critical operations.

To address the protection of these critical systems, IAIP has developed a comprehensive strategy to protect each element of process control systems. Our focus is on joint government-industry efforts to identify key assets, discover vulnerabilities, analyze risk, implement effective protective measures, conduct joint exercises and training, disseminate information, and develop inherently safer technology. Since most process control systems reside in the private sector, our ability to always effect change are sometimes affected by business factors that we cannot control.

IAIP manages this as a team effort that includes all parts of the Directorate, including PSD, the National Cyber Security Division (NCSD), the Infrastructure Coordination Division (ICD), and the National Communication System (NCS). The bulk of the remediation and protective activities are conducted by PSD and NCSD. To support these efforts, the Assistant Secretary for Information Analysis (IA), the intelligence arm of IAIP, along with the Office of Science and Technology, Office of State and Local Government Coordination, and the Office of Private Sector Liaison, provide the Office of Infrastructure Protection (IP) with crucial information and assistance. Beyond the Department, we are coordinating protection activities with the Department of Defense, the Department of Energy, and others. We are working on international partnership with Canada as it relates to the control systems of the North American electric grid.

In order to put this into perspective, I would like to briefly explain our overall operational philosophy. The overarching principle is to “Detect, Deter, Devalue, and Defend.”

How do we do this?

- Through the deployment of specialized teams of security specialists to conduct site assist visits (SAVs), to evaluate vulnerability and establish whether or not site protection plans adequately address real-world security concerns.
- Through the development of community-based buffer zone protection plans (BZPP), that recognize that security does not end at the fence-line, and that local law enforcement and emergency responders are as integral to security as onsite personnel and equipment.
- Through third party submissions, including information provided from other Federal agencies, State and local governments, and private sector entities.
- Through special penetration testing of systems.

Immediate efforts focus on protective measures that can be implemented within the as-installed/legacy environment, such as inexpensive technical or procedural changes that can be implemented at the site and in the immediate future. Near term efforts include detailed testing and assessment of the vulnerabilities of PCS. In the long-term, we will work with the private sector on the development of inherently safer technology.

As part of PSD, we have established a Control Systems Section (CSS) that oversees the PCS Security program. CSS will identify and reduce vulnerabilities critical to domestic security related to PCS. This Section also includes the development and integration of the understanding of offensive capabilities, and providing relevant “hands on” operational support during DHS heightened security events.

PSD has identified approximately 1,700 facilities across the country that we hope to engage in a major vulnerability reduction effort during FY04. Of those sites, we have identified roughly 565 with process control systems. As appropriate, reduction in SCADA vulnerabilities will be undertaken just as reductions in physical vulnerabilities are.

Additionally, community-based Buffer Zone Protection Plans (BZPPs) that are being developed will incorporate protective measures for critical process control system sites. BZPPs, created through a collaborative effort between DHS, owners/operators, local governments, the law enforcement community, and other stakeholders, further strengthen identified sites by addressing the vulnerabilities of the larger community.

While PSD is working on vulnerability reduction at specific critical sites, NCS is working the problem from a more global perspective. NCS is holding meetings with industry experts to discuss in general terms vulnerabilities in a given critical infrastructure, participating in industry and government sponsored working groups, and directly engaging sector-specific Federal agencies, and State and local governments.

NCS also analyzes and shares threat information of a cyber nature with all branches of government and industry. The Strategic Programs Section within NCS routinely reaches out to industry, academia, and sector specific agencies to coordinated cyber protection activities.

Also, NCS is performing communications modeling of SCADA systems in partnership with Idaho National Engineering and Environmental Lab (INEEL). INEEL is the lead lab for the National SCADA Test Bed which is funded as part of the Critical Infrastructure Protection Test Range by PSD. The NCS Advanced Technology Branch has initiated a study to look at the SCADA vulnerabilities of the natural gas transmission systems serving the U. S. eastern seaboard and efforts are underway to identify the high power microwave vulnerabilities of commercial SCADA systems.

PSD and NCS are actively participating with industry sponsored groups like the North American Electric Reliability Council's (NERC) Process Control Systems Security Task Force and the National Institute of Standards and Technology's (NIST) working group on process control systems security.

All of these activities will contribute to more comprehensive risk assessments of process control systems, including systems and component testing; will produce a refined, prioritized list of sites and vulnerabilities along with recommendations for effective protective measures.

In the long-term, targeted PCS security improvements will result in PCS architectures that are, by design, more inherently secure. This will be accomplished by ongoing partnerships with National Laboratories, owners and operators, and manufacturers.

In closing, I would like to reiterate first that SCADA vulnerabilities are a fact, just like a hole in a perimeter fence. The problem is that the SCADA vulnerability is not seen by the casual observer and therefore can easily go unnoticed. SCADA vulnerabilities are seen by those who would do us harm through their manipulation and it is incumbent upon IAIP to ensure that those responsible for protecting America are seeing them and doing something about it. Finally, as stated earlier, the Department of Homeland Security views

this as a national effort involving many directorates within the Department and many organizations, both public and private, outside of DHS.

I would be happy to answer questions you might have.