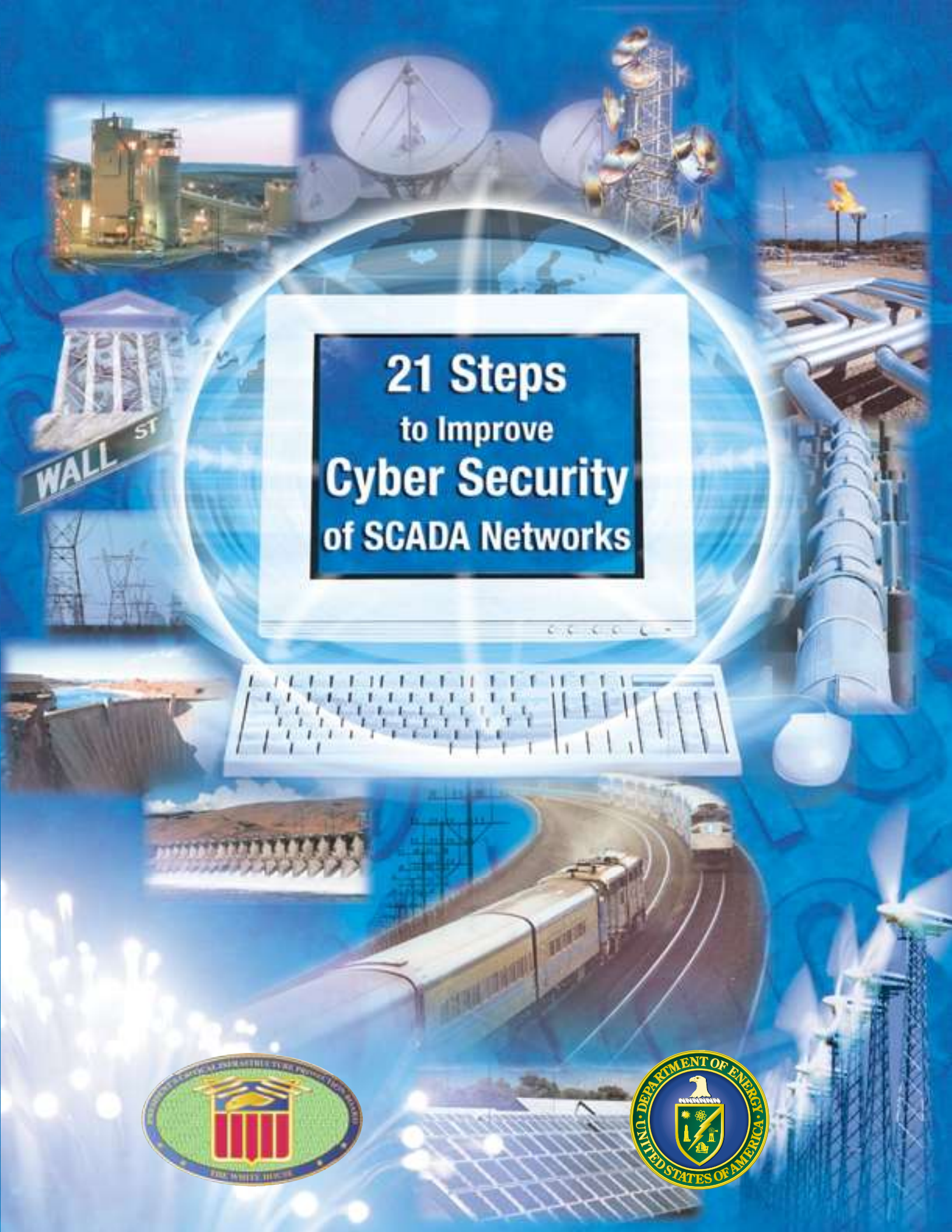
21 Steps
to Improve
Cyber Security
of SCADA Networks
WALL ST
DEPARTMENT OF ENERGY
UNITED STATES OF AMERICA

Table of Contents

21 Steps to Improve Cyber Security of SCADA Networks

Introduction

Supervisory control and data acquisition (SCADA) networks contain computers and applications that perform key functions in providing essential services and commodities (e.g., electricity, natural gas, gasoline, water, waste treatment, transportation) to all Americans. As such, they are part of the nation's critical infrastructure and require protection from a variety of threats that exist in cyber space today. By allowing the collection and analysis of data and control of equipment such as pumps and valves from remote locations, SCADA networks provide great efficiency and are widely used. However, they also present a security risk. SCADA networks were initially designed to maximize functionality, with little attention paid to security. As a result, performance, reliability, flexibility and safety of distributed control/SCADA systems are robust, while the security of these systems is often weak. This makes some SCADA networks potentially vulnerable to disruption of service, process redirection, or manipulation of operational data that could result in public safety concerns and/or serious disruptions to the nation's critical infrastructure. Action is required by all organizations, government or commercial, to secure their SCADA networks as part of the effort to adequately protect the nation's critical infrastructure.

The President's Critical Infrastructure Protection Board, and the Department of Energy, have developed the steps outlined here to help any organization improve the security of its SCADA networks. These steps are not meant to be prescriptive or all-inclusive. However, they do address essential actions to be taken to improve the protection of SCADA networks. The steps are divided into two categories: specific actions to improve implementation, and actions to establish essential underlying management processes and policies.

Background

President Bush created the President's Critical Infrastructure Protection Board in October 2001 through Executive Order 13231 to coordinate all Federal activities related to the protection of information systems and networks supporting critical infrastructures, including:

- Federal departments and agencies
- Private Sector companies that operate critical infrastructures
- State and local government's critical infrastructures
- Related national security programs.

The Department of Energy plays a key role in protecting the critical energy infrastructure of the nation as specified in the National Strategy for Homeland Security. In fulfilling this responsibility, the Secretary of Energy's Office of Independent Oversight and Performance Assurance has conducted a number of assessments of organizations with SCADA networks to develop an in-depth understanding of SCADA networks and steps necessary to secure these networks. The Office of Energy Assurance also fulfills Energy Department responsibilities through their work with Federal, State, and private partners to protect the National Energy Infrastructure, improve energy reliability, and assist in energy emergency response efforts.

The following steps focus on specific actions to be taken to increase the security of SCADA networks:

1. Identify all connections to SCADA networks.

Conduct a thorough risk analysis to assess the risk and necessity of each connection to the SCADA network. Develop a comprehensive understanding of all connections to the SCADA network, and how well these connections are protected. Identify and evaluate the following types of connections:

- Internal local area and wide area networks, including business networks
- The Internet
- Wireless network devices, including satellite uplinks
- Modem or dial-up connections
- Connections to business partners, vendors or regulatory agencies

2. Disconnect unnecessary connections to the SCADA network.

To ensure the highest degree of security of SCADA systems, isolate the SCADA network from other network connections to as great a degree as possible. Any connection to another network introduces security risks, particularly if the connection creates a pathway from or to the Internet. Although direct connections with other networks may allow important information to be passed efficiently and conveniently, insecure connections are simply not worth the risk; isolation of the SCADA network must be a primary goal to provide needed protection. Strategies such as utilization of "demilitarized zones" (DMZs) and data warehousing can facilitate the secure transfer of data from the SCADA network to business networks. However, they must be designed and implemented properly to avoid introduction of additional risk through improper configuration.

3. Evaluate and strengthen the security of any remaining connections to the SCADA network.

Conduct penetration testing or vulnerability analysis of any remaining connections to the SCADA network to evaluate the protection posture associated with these pathways. Use this information in conjunction with risk management processes to develop a robust protection strategy for any pathways to the SCADA network. Since the SCADA network is only as secure as its weakest connecting point, it is essential to implement firewalls, intrusion detection systems (IDSs), and other appropriate security measures at each point of entry. Configure firewall rules to prohibit access from and to the SCADA network, and be as specific as possible when permitting approved connections. For example, an Independent System Operator (ISO) should not be granted "blanket" network access simply because there is a need for a connection to certain components of the SCADA system. Strategically place IDSs at each entry point to alert security personnel of potential breaches of network security. Organization management must understand and accept responsibility for risks associated with any connection to the SCADA network.

4. Harden SCADA networks by removing or disabling unnecessary services.

SCADA control servers built on commercial or open-source operating systems can be exposed to attack through default network services. To the greatest degree possible, remove or disable unused services and network daemons to reduce the risk of direct attack. This is particularly important when SCADA networks are interconnected with other networks. Do not permit a service or feature on a SCADA network unless a thorough risk assessment of the consequences of allowing the service/feature shows that the benefits of the service/feature far outweigh the potential for vulnerability exploitation. Examples of services to remove from SCADA networks include automated meter reading/remote billing systems, email services, and Internet access. An example of a feature to disable is remote maintenance. Numerous secure configuration guidelines for both commercial and open source operating systems are in the public domain, such as the National Security Agency's series of security guides. Additionally, work closely with SCADA vendors to identify secure configurations and coordinate any and all changes to operational systems to ensure that removing or disabling services does not cause downtime, interruption of service, or loss of support.

5. Do not rely on proprietary protocols to protect your system.

Some SCADA systems use unique, proprietary protocols for communications between field devices and servers. Often the security of SCADA systems is based solely on the secrecy of these protocols. Unfortunately, obscure protocols provide very little "real" security. Do not rely on proprietary protocols or factory default configuration settings to protect your system. Additionally, demand that vendors disclose any backdoors or vendor interfaces to your SCADA systems, and expect them to provide systems that are capable of being secured.

6. Implement the security features provided by device and system vendors.

Most older SCADA systems (most systems in use) have no security features whatsoever. SCADA system owners must insist that their system vendor implement security features in the form of product patches or upgrades. Some newer SCADA devices are shipped with basic security features, but these are usually disabled to ensure ease of installation.

Analyze each SCADA device to determine whether security features are present. Additionally, factory default security settings (such as in computer network firewalls) are often set to provide maximum usability, but minimal security. Set all security features to provide the maximum level of security. Allow settings below maximum security only after a thorough risk assessment of the consequences of reducing the security level.

7. Establish strong controls over any medium that is used as a backdoor into the SCADA network.

Where backdoors or vendor connections do exist in SCADA systems, strong authentication must be implemented to ensure secure communications. Modems, wireless, and wired networks used for communications and maintenance represent a significant vulnerability to the SCADA network and remote sites. Successful "war dialing" or "war driving" attacks could allow an attacker to bypass all other controls and have direct access to the SCADA network or resources. To minimize the risk of such attacks, disable inbound access and replace it with some type of callback system.

8. Implement internal and external intrusion detection systems and establish 24-hour-a-day incident monitoring.

To be able to effectively respond to cyber attacks, establish an intrusion detection strategy that includes alerting network administrators of malicious network activity originating from internal or external sources. Intrusion detection system monitoring is essential 24 hours a day; this capability can be easily set up through a pager. Additionally, incident response procedures must be in place to allow an effective response to any attack. To complement network monitoring, enable logging on all systems and audit system logs daily to detect suspicious activity as soon as possible.

9. Perform technical audits of SCADA devices and networks, and any other connected networks, to identify security concerns.

Technical audits of SCADA devices and networks are critical to ongoing security effectiveness. Many commercial and open-source security tools are available that allow system administrators to conduct audits of their systems/networks to identify active services, patch level, and common vulnerabilities. The use of these tools will not solve systemic problems, but will eliminate the "paths of least resistance" that an attacker could exploit. Analyze identified vulnerabilities to determine their significance, and take corrective actions as appropriate. Track corrective actions and analyze this information to identify trends. Additionally, retest systems after corrective actions have been taken to ensure that vulnerabilities were actually eliminated. Scan non-production environments actively to identify and address potential problems.

10. Conduct physical security surveys and assess all remote sites connected to the SCADA network to evaluate their security.

Any location that has a connection to the SCADA network is a target, especially unmanned or unguarded remote sites. Conduct a physical security survey and inventory access points at each facility that has a connection to the SCADA system. Identify and assess any source of information including remote telephone/computer network/fiber optic cables that could be tapped; radio and microwave links that are exploitable; computer terminals that could be accessed; and wireless local area network access points. Identify and eliminate single points of failure. The security of the site must be adequate to detect or prevent unauthorized access. Do not allow "live" network access points at remote, unguarded sites simply for convenience.

11. Establish SCADA "Red Teams" to identify and evaluate possible attack scenarios.

Establish a "Red Team" to identify potential attack scenarios and evaluate potential system vulnerabilities. Use a variety of people who can provide insight into weaknesses of the overall network, SCADA systems, physical systems, and security controls. People who work on the system every day have great insight into the vulnerabilities of your SCADA network and should be consulted when identifying potential attack scenarios and possible consequences. Also, ensure that the risk from a malicious insider is fully evaluated, given that this represents one of the greatest threats to an organization. Feed information resulting from the "Red Team" evaluation into risk management processes to assess the information and establish appropriate protection strategies.

The following steps focus on management actions to establish an effective cyber security program:

12. Clearly define cyber security roles, responsibilities, and authorities for managers, system administrators, and users.

Organization personnel need to understand the specific expectations associated with protecting information technology resources through the definition of clear and logical roles and responsibilities. In addition, key personnel need to be given sufficient authority to carry out their assigned responsibilities. Too often, good cyber security is left up to the initiative of the individual, which usually leads to inconsistent implementations and ineffective security. Establish a cyber security organizational structure that defines roles and responsibilities and clearly identifies how cyber security issues are escalated and who is notified in an emergency.

13. Document network architecture and identify systems that serve critical functions or contain sensitive information that require additional levels of protection.

Develop and document a robust information security architecture as part of a process to establish an effective protection strategy. It is essential that organizations design their networks with security in mind and continue to have a strong understanding of their network architecture throughout its lifecycle. Of particular importance, an in-depth understanding of the functions that the systems perform and the sensitivity of the stored information is required. Without this understanding, risk cannot be properly assessed and protection strategies may not be sufficient. Documenting the information security architecture and its components is critical to understanding the overall protection strategy, and identifying single points of failure.

14. Establish a rigorous, ongoing risk management process.

A thorough understanding of the risks to network computing resources from denial-of-service attacks and the vulnerability of sensitive information to compromise is essential to an effective cyber security program. Risk assessments form the technical basis of this understanding and are critical to formulating effective strategies to mitigate vulnerabilities and preserve the integrity of computing resources. Initially, perform a baseline risk analysis based on a current threat assessment to use for developing a network protection strategy. Due to rapidly changing technology and the emergence of new threats on a daily basis, an ongoing risk assessment process is also needed so that routine changes can be made to the protection strategy to ensure it remains effective. Fundamental to risk management is identification of residual risk with a network protection strategy in place and acceptance of that risk by management.

15. Establish a network protection strategy based on the principle of defense-in-depth.

A fundamental principle that must be part of any network protection strategy is defense-in-depth. Defense-in-depth must be considered early in the design phase of the development process, and must be an integral consideration in all technical decision-making associated with the network. Utilize technical and administrative controls to mitigate threats from identified risks to as great a degree as possible at all levels of the network. Single

points of failure must be avoided, and cyber security defense must be layered to limit and contain the impact of any security incidents. Additionally, each layer must be protected against other systems at the same layer. For example, to protect against the insider threat, restrict users to access only those resources necessary to perform their job functions.

16. Clearly identify cyber security requirements.

Organizations and companies need structured security programs with mandated requirements to establish expectations and allow personnel to be held accountable. Formalized policies and procedures are typically used to establish and institutionalize a cyber security program. A formal program is essential for establishing a consistent, standards-based approach to cyber security throughout an organization and eliminates sole dependence on individual initiative. Policies and procedures also inform employees of their specific cyber security responsibilities and the consequences of failing to meet those responsibilities. They also provide guidance regarding actions to be taken during a cyber security incident and promote efficient and effective actions during a time of crisis. As part of identifying cyber security requirements, include user agreements and notification and warning banners. Establish requirements to minimize the threat from malicious insiders, including the need for conducting background checks and limiting network privileges to those absolutely necessary.

17. Establish effective configuration management processes.

A fundamental management process needed to maintain a secure network is configuration management. Configuration management needs to cover both hardware configurations and software configurations. Changes to hardware or software can easily introduce vulnerabilities that undermine network security. Processes are required to evaluate and control any change to ensure that the network remains secure. Configuration management begins with well-tested and documented security baselines for your various systems.

18. Conduct routine self-assessments.

Robust performance evaluation processes are needed to provide organizations with feedback on the effectiveness of cyber security policy and technical implementation. A sign of a mature organization is one that is able to self-identify issues, conduct root cause analyses, and implement effective corrective actions that address individual and systemic problems. Self-assessment processes that are normally part of an effective cyber security program include routine scanning for vulnerabilities, automated auditing of the network, and self-assessments of organizational and individual performance.

19. Establish system backups and disaster recovery plans.

Establish a disaster recovery plan that allows for rapid recovery from any emergency (including a cyber attack). System backups are an essential part of any plan and allow rapid reconstruction of the network. Routinely exercise disaster recovery plans to ensure that they work and that personnel are familiar with them. Make appropriate changes to disaster recovery plans based on lessons learned from exercises.

20. Senior organizational leadership should establish expectations for cyber security performance and hold individuals accountable for their performance.

Effective cyber security performance requires commitment and leadership from senior managers in the organization. It is essential that senior management establish an expectation for strong cyber security and communicate this to their subordinate managers throughout the organization. It is also essential that senior organizational leadership establish a structure for implementation of a cyber security program. This structure will promote consistent implementation and the ability to sustain a strong cyber security program. It is then important for individuals to be held accountable for their performance as it relates to cyber security. This includes managers, system administrators, technicians, and users/operators.

21. Establish policies and conduct training to minimize the likelihood that organizational personnel will inadvertently disclose sensitive information regarding SCADA system design, operations, or security controls.

Release data related to the SCADA network only on a strict, need-to-know basis, and only to persons explicitly authorized to receive such information. "Social engineering," the gathering of information about a computer or computer network via questions to naive users, is often the first step in a malicious attack on computer networks. The more information revealed about a computer or computer network, the more vulnerable the computer/network is. Never divulge data related to a SCADA network, including the names and contact information about the system operators/administrators, computer operating systems, and/or physical and logical locations of computers and network systems over telephones or to personnel unless they are explicitly authorized to receive such information. Any requests for information by unknown persons need to be sent to a central network security location for verification and fulfillment. People can be a weak link in an otherwise secure network. Conduct training and information awareness campaigns to ensure that personnel remain diligent in guarding sensitive network information, particularly their passwords.

For further information, please contact:

The President's Critical Infrastructure Protection Board

Office of Energy Assurance
U.S. Department of Energy

202/287-1808

Office of Independent Oversight and Performance Assurance
U.S. Department of Energy

301/903-3777