INEEL/EXT-04-02264

Control Systems Security and Test Center

Personnel Security Guidelines

Prepared by the Idaho National Engineering and Environmental Laboratory

September 30, 2004

INEEL/EXT-04-02264

Personnel Security Guidelines

September 30, 2004

Control Systems Security and Test Center
Idaho Falls, Idaho 83415

Prepared for the
U.S. Department of Homeland Security
Under DOE Idaho Operations Office
Contract DE-AC07-99ID13727

ABSTRACT

Many vital industries and critical infrastructures depend heavily on automated control systems. An effective personnel security program that addresses post-9/11 threats is necessary to ensure that personnel working with control systems are indeed trustworthy, capable, and operationally safe.

The largest blackout ever to occur in the United States has been attributed to a lack of personnel capability and training, as well as poor communication and faulty equipment, and the blackout investigation taskforce recommended mandatory government regulation, oversight, and penalties for violation. Human performance issues contributed to the severity of the August 14th blackout. However, various industry and government groups currently offer personnel security guidance. This document offers personnel security program guidance based on recommendations from seven nationally recognized industry and government groups.

Guidance offered in this document addresses three broad areas related to personnel security: trustworthiness, capability, and operationally safe environments. Trustworthiness includes background investigation; physical, mental, and psychological qualifications; behavioral observation; and voluntary and continuing assessments. Capability addresses education and experience; training (equipment-specific, initial, and ongoing); security awareness; and certification by examination. Operationally safe environments addresses vulnerability and risk assessment; hierarchy; internal, external, and contractor/vendor audits and enforcement; emergency planning; control system access control; identification and authentication; and emergency communication.

Recruiting and screening trustworthy, capable, and safe individuals to secure control systems is vital, and the personnel security guidance in this document is broadly applicable. However, these personnel security guidelines are general; specific personnel security programs should be based on facility size, location, type, and existing security measures. Organizations should recognize and respond to the responsibility to protect their workers, communities, and supply/distribution networks through a variety of security based standards and procedures.

CONTENTS

TABLE

ACRONYMS

API	American Petroleum Institute
CCST	Certified Control System Technician
CFR	Code of Federal Regulations
CIDX	Chemical Industry Data Exchange
CNN	Cable News Network
DHS	Department of Homeland Security
DOE	Department of Energy
EPA	Environmental Protection Agency
ID	Identification
ISA	Instrument Society of America
NERC	National Electric Reliability Council
NRC	Nuclear Regulatory Commission
SDWA	Safe Drinking Water Act
SVA	Site Vulnerability Assessment
U.S.	United States

1. INTRODUCTION

This document was prepared by the Control System Security and Test Center (CSSTC) as part of the Near-term Center Operations Task, Control Systems Personnel Security Guidance. The purpose of the task was to compare the personnel security guidance of major industries and government agencies and, based on prior practice, develop a set of guidelines for use by critical infrastructure facilities with significant reliance on cyber-related control systems. This task supports Goal 4 of the US-CERT National Strategy for Control Systems Security which, in part, seeks "awareness of the issues and education on insecure practices (to) form the basis of improved practices and a foundation for sound security policy."

Introduction

- Organizations depend heavily on automated control systems.
- Trustworthy, capable, operationally safe personnel are vital to safe control system operation.
- Some organizations may need to update their personnel security program to reflect post-9/11 threats.
- This document offers personnel security program guidance based on recommendations from seven nationally recognized industry and government groups.

Obtaining trustworthy, capable, and operationally safe individuals to secure and operate an organization's control systems is of vital importance; personnel security programs are a top concern. An organization, as used in this document, is a group of people who work together in a company, corporation, firm, enterprise, or institution, or part or combination thereof, whether incorporated or not, public or private, that has its own functions and administration. Vital national industries such as oil and gas refineries and distribution systems, chemical plants, and similar industrial facilities, as well as infrastructures such as electrical generation and distribution facilities and transportation infrastructures are examples of organizations that rely heavily on control systems and organizations in which control system security is a major concern.

Organizations depend on control systems to sustain security, maintain economic operation, protect the public health and safety, and protect the environment. Control systems are part of a crucial infrastructure that monitors and controls critical industries. Control systems are only as secure as the people who operate them. Since September 11, 2001, many organizations have been reevaluating personnel security programs based on each individual's responsibilities. It is imperative that organizations recognize new threats posed by intentional acts motivated by changing world political and social conditions.

In response to the new threats, some organizations may need to implement or update a personnel security program to prevent unauthorized access to control systems and critical information. Organizations should develop specific trustworthiness and capability criteria for personnel security and control system integrity. The personnel security program should consider an individual's background, qualifications, and operational restrictions prior to granting an individual access to protected information and control rooms. The overall objective is to ensure that individuals granted access are trustworthy, capable, and operationally safe. Also, the organization, including the employees and the environment in which they function, should operate securely so that they do not constitute an unacceptable security risk that could impact the health and safety of other personnel or the public.

This document offers recommendations and guidelines for personnel security programs based on review and analysis of personnel security practices promoted by seven nationally recognized organizations:

- The Instrumentation, Systems, and Automation Society (ISA)
- Nuclear Regulatory Commission (NRC)
- Department of Energy (DOE)
- Environmental Protection Agency (EPA)
- North American Electric Reliability Council (NERC)
- American Petroleum Institute (API)
- Chemical Industry Data Exchange (CIDX).

This document is organized around three principal concepts: trustworthiness, capability, and a secure environment. For the purposes of this guidance, they are defined as follows:

- Trustworthiness is a measure of reliability, integrity, and character, used as a metric that ensures that individuals are not a security threat to secure operations.
- Capability ensures that individuals are trained, skilled, and possess the necessary knowledge and understanding of the personnel security program and the technical requirements of their assigned work scope.
- A secure environment broadly includes the control system, the operator, good management practices, and the security restrictions that are in place to ensure safe day-to-day operations, and it assumes that trustworthy and capable operators are in place.

1.1 Applicability

This guideline is intended for use by organizations and recommends security practices that organizations should apply to control system personnel, including operators that have direct access to control systems in facilities. Organizations may choose to accept a personnel security program used by a contractor, subcontractor, or vendor; but they should meet the requirements of these guidelines by either substituting, supplementing, or duplicating any portion of the program necessary to meet this guidance.

Organizations are responsible for granting, denying, or revoking unescorted access authorization to any contractor, vendor, or other affected control system personnel. The specifically recommended guidelines are grouped in the following areas:

1. Trustworthiness
2. Capability
3. Secure environment.

2. BACKGROUND

Background

- The largest blackout to occur in the United States has been attributed to a lack of personnel capability and training.
- The blackout investigation taskforce recommended mandatory government regulation, oversight, and penalties for violation.
- Industry and government oversight organizations have published personnel security recommendations.
- Some organizations have updated their personnel security plans, but others have not.

On August 14, 2003, the largest ever electricity blackout hit the United States. Its widespread economic damage affected areas in Ohio, Michigan, Pennsylvania, New York, New Jersey, Vermont, Massachusetts, Connecticut, and Ontario province. A task force was assembled to investigate the cause and make recommendations aimed at preventing blackouts. An article was posted 5/18/04 on CNN's website (www.cnn.com) where the task force blamed "FirstEnergy Corporation, based in Akron, Ohio, for the electrical failures on August 14, faulting the company's lack of communication, faulty equipment and inadequate training." The task force recommended the need for mandatory reliability regulations with government oversight and penalties for noncompliance, but "the power industry now has voluntary requirements… …administered by the private North American Electric Reliability Council, which lacks the ability to hand down penalties." In addition, the task force's specific recommendations included "Improving training and certification requirements for operators, reliability coordinators, and support staff," and "Increasing the network's physical and cyber security" (Blackout was preventable…). The economic impact of the blackout is estimated at about $6 billion, as published by the DOE (Transforming the Grid…). Human performance issues contributed to the severity of the August 14th blackout.

Organizations have long recognized the requirement to protect control systems through a variety of guidelines. Various organizations' personnel security plans were reviewed because they currently have personnel security guidelines in place. They currently have a security focus for safeguarding their control systems against domestic and international terrorism. Each of these organizations have taken an approach to: assess the types of risk associated with the public, workers, the environment, and economic production; and identify guidance to mitigate risks and/or vulnerabilities. In preparing this report, the Department of Homeland Security (DHS) has reviewed current guidance documents from the following organizations that pertain to control system personnel:

- American Petroleum Institute (API)
  - The API owns the nation's petroleum and gas facilities and is voluntarily taking actions to protect and secure their assets. They have a vested and economic interest in commercial operations and facility availability. The API is made up of employees from various commercial organizations and has the authority to penalize for noncompliance.
  - The API's mission is to influence public policy in support of a strong, viable U.S. oil and natural gas industry essential to meet the needs of consumers in an efficient, environmentally responsible manner.
- Chemical Industry Data Exchange (CIDX)
  - The CIDX comprises senior executives from the companies participating in the global chemical sector value chain and is voluntarily taking actions to protect and secure their

assets. They have a vested and economic interest in commercial operations and facility availability. The CIDX is made up of employees from various commercial organizations and has the authority to penalize for noncompliance.

  - The CIDX's mission is to improve the ease, speed, and cost of conducting business between chemical companies and their trading partners.

- Nuclear Regulatory Commission (NRC)
  - The NRC regulates nuclear reactors, materials, and waste and requires civilian users of nuclear materials and facilities to comply with requirements issued by Code of Federal Regulations (CFR) Section 10, acts, by-laws, and policies. The NRC is made up of U.S. government employees that are not civilian nuclear facility employees and has the authority to penalize for noncompliance.
  - The NRC's mission is to regulate the nation's civilian use of byproduct, source, and special nuclear materials to ensure adequate protection of public health and safety, to promote the common defense and security, and to protect the environment.
- Department of Energy (DOE)
  - The DOE regulates all DOE elements and facilities to comply with requirements issued by cognizant DOE offices, Headquarters, Headquarters Operations Division, and the Office of Safeguards and Security. The DOE is made up of U.S. government employees that oversee DOE facilities and has the authority to penalize for noncompliance.
  - The DOE's mission is to advance the national economic and energy security of the U.S.; to promote scientific and technological innovation in support of that mission; to ensure the environmental cleanup of the national nuclear weapons complex; and to protect our national security.
- Environmental Protection Agency (EPA)
  - The EPA regulates every organization and requires compliance with CFR Section 40, acts, by-laws, and policies. The EPA is made up of U.S. government employees that oversee every organization and has the authority to penalize for noncompliance.
  - The EPA's mission is to protect human health and the environment.
- North American Electric Reliability Council (NERC)
  - The NERC advises the electricity sector and offers guidance to be applied in protecting electric infrastructure systems. The NERC operates as a voluntary, not-for-profit organization that relies on industry self interest and does not have the authority to penalize for noncompliance.
  - NERC's mission is to ensure that the bulk electric system is reliable, adequate, and secure.
- The Instrumentation, Systems, and Automation Society (ISA)
  - The ISA advises the control system sector and offers guidance and training to improve security. The ISA operates as a voluntary, not-for-profit, educational organization that relies on industry self interest and does not have the authority to penalize for noncompliance.
  - The ISA's mission is to maximize the effectiveness of practitioners and organizations worldwide to advance and apply the science, technology, and allied arts of instrumentation, systems, and automation in all industries and applications.

3. SPECIFIC RECOMMENDED GUIDELINES

3.1 Trustworthiness

Background Investigation

Organizations should require individuals to complete verification of employment forms for all prior employers or provide equivalent documentation that contains all information on the verification of employment forms in a clear and readable format. The following full contact information for all responsible parties who act to confirm employment verification should be provided:

- Name
- Address
- Telephone number
- Position description from that period of employment
- Their present company name, telephone, and address.

Specific Guidelines

- Trustworthiness
  - Background investigation
  - Physical, mental, psychological qualifications
  - Behavioral observation
  - Voluntary and continuing assessments.
- Capability
  - Education and experience
  - Training (equipment-specific, initial, and ongoing)
  - Security awareness
  - Certification by examination.
- Secure Environment
  - Vulnerability and risk assessment
  - Hierarchy
  - Internal, external, and contractor/vendor audits
  - Enforcement
  - Emergency plan
  - Control system access control
  - Identification and authentication.

Depending on the security access required, organizations should require that the individual's former supervisor sign all forms. For employers that may be unavailable to provide first-hand verification, a two-party verification of the employment should be provided in the form of a statement signed by a co-worker from that period of employment and notarized by a notary public. In addition, a full explanation of why the employer is not verifying the period of employment should be provided. All documents should be kept as permanent records. At a minimum, the background investigation should verify the following:

- History of convictions for theft or violent crimes
- Arrests
- Workplace violence or threatening behavior
- Individual identification
- Employment history
- Education
- Criminal record
- Motor vehicle record
- Credit history
- Military history

- Professional accreditations
- Negative drug test results.

Physical Qualifications

Operators should pass a physical examination administered by a licensed physician. The examination should be designed to measure the individual's physical ability to perform assigned job duties, as identified in the organization's job qualification program.

Mental Qualifications

Individuals whose job duties are directly associated with the effective implementation of the organization's process controls should demonstrate mental alertness and the capability to exercise good judgment, execute instructions, and assimilate assigned tasks. These individuals should possess acuity of senses and ability of expression sufficient to permit accurate communication by written, spoken, audible, visible, or other signals required by assigned job duties. Individuals should have no established medical history or medical diagnosis of epilepsy or diabetes or, where such a condition exists, the individual should provide medical evidence that the condition can be controlled with proper medication so that the individual will not lapse into a coma or unconscious state while performing assigned job duties.

Psychological Qualifications

Organizations should be required to evaluate the possible impact of any noted psychological characteristics that may have a bearing on trustworthiness. Control system operators should have no emotional instability or affiliations with organizations that pose a threat to security that would interfere with the effective performance of assigned job duties. This determination should be made by a licensed psychologist, psychiatrist, physician, or any other person professionally trained to identify emotional instability.

Behavioral Observation

Organizations should be required to observe individual behavioral changes which, if left unattended, could lead to acts detrimental to the public health and safety. Individuals should have no established medical history or medical diagnosis of habitual alcoholism or drug addiction or, when such a condition has existed, the individual should provide certified documentation of having completed a rehabilitation program that would give a reasonable degree of confidence that the individual is capable of performing assigned job duties.

Voluntary Assessment

Organizations should give an individual an opportunity to report any information concerning authorization and security to perform assigned job duties.

Continuing Assessment

Organizations should arrange for continued observation of individuals and for appropriate corrective measures by responsible supervisors for indications of emotional instability of individuals in the course of performing assigned security job duties. Identification of emotional instability reported by responsible supervisors should be subject to verification by a licensed, trained person.

3.2 Capability

Education and Experience

Individuals should be required to possess a high school diploma or pass an equivalent performance examination designed to measure basic job-related mathematical, language, and reasoning skills, as well as the ability and knowledge required by assigned job duties. Individuals should be required to have the defined minimum amount of on-the-job experience for each appropriate level of operator certification required by their assigned job duties, as defined by the employer.

Training

Each individual who requires training to perform assigned job tasks or job duties as identified by the organization's operating or contingency plans should, prior to assignment, be trained to perform those tasks and duties in accordance with the organization's documented training and qualification plan. Individuals should be required to have the defined amount of training for each appropriate level of operator certification. Operators should receive training in specialized subjects such as:

- Theory of control
- Analog and digital electronics
- Microprocessors and computers
- Operation and maintenance of particular lines of field instrumentation
- Electrical fundamentals
- Vendor certification on proprietary equipment.

Where applicable, organizations should require training on equipment that measures and controls:

- Level
- Temperature
- Pressure
- Flow
- Force
- Power
- Position
- Motion
- Physical properties
- Chemical composition.

Security Awareness

Each individual should receive ongoing employee awareness sessions and training. The individual's role in providing protection for the organization should include training in the following subjects:

- Adversary group operations

- Motivation and objectives of adversary groups
- Tactics and force that might be used by adversary groups to achieve their objectives
- Recognition of sabotage-related devices and equipment that might be used against the organization's facility or shipment vehicle
- Facility security organization and operation
- Types of physical and cyber security barriers
- Weapons that might be used by adversary groups to achieve their objectives
- Lock and key control system barriers
- Potential vulnerability and consequences of sabotage of a facility
- Types of alarm systems used
- Protection of control system information
- Access control system operation
- Contingency response to confirmed intrusion or attempted intrusion
- Control system operation after component failure
- Social engineering, unauthorized inquiries to illicit secure information such as passwords, network design, process descriptions, or schematics.

Ongoing Training

Organizations should be required to remain current with changes in technology to understand new advances. Organizations should require an individual to recertify if the individual fails to renew or qualify for renewal after the date that the certification has expired. The organization should establish training requirements for certification renewal and expiration based on the level of certification held by the operator. Organizations should have a process for recertification of individuals whose certification has expired. The process should include review of the individual's experience and training and reexamination.

Certification Exams

Individuals should be certified before being allowed to operate controls systems. Certification should require that the individual attain a passing score on an examination that tests the individuals knowledge of the following topics:

- Calibration
- Loop Checking
- Troubleshooting
- Maintenance/Repair
- Project Organization
- Proprietary Systems.

Examinations consisting of multiple-choice questions and written problems that test the candidate's ability to apply the knowledge and skills required for each subject are recommended.

3.3 Secure Environment

Vulnerability and Risk Assessment

An organization should require a Security Vulnerability Assessment (SVA) process to assess risks and make decisions about operating risks, and to make progress towards the goal of reducing the risks associated with control system operations. The SVA will identify and analyze the following:

- Actual and potential precursor events that can result in control system-related incidents
- The likelihood and consequence of potential control system-related events
- A comprehensive and integrated means for examining and comparing the spectrum of risks and risk reduction activities available
- A structured, easily communicated means for selecting and implementing risk reduction activities
- A means of tracking program performance with the goal of improving the SVA process
- A means of establishing a communications program to share threat information between federal agencies and organizations.

In addition, each organization should assess the risk of a terrorist attack. The assessment should include a determination of the likelihood of an act or attack, the type of terrorist action, and consequences, depending on the size and location of the system. The assessment should include potential risks to the following:

- Workers
- Environment and surrounding community
- Impact to the local, regional and national economics
- Adjacent and/or interdependent facilities and infrastructure.

A key element of the security management framework is the integration of all available information into the decision making process. Information that can impact an operator's understanding of the important risks to a control system comes from a variety of sources. The operator is in the best position to gather and analyze this information. By integrating available information, the operator can assist in determining where the risk of an incident is the greatest and support prudent decisions to reduce the risk.

Another consideration should be closely safeguarding such information and restricting it to only a few individuals with a "need to know." Vulnerability analyses and risk assessments provide a method of prioritizing the criticality of assets (or the impact of the loss of the asset), threats, and countermeasure strategies. In many cases, a checklist survey is used in conducting a risk and vulnerability assessment. The checklist includes an overview of a fairly standard approach to concepts of risk assessment, and includes questions and considerations for use during each step of the process. The assessment helps identify those facilities that may be critical to overall operations, as well as their vulnerabilities.

Hierarchy

Individuals should be certified to a standard equal to or greater than the classification of the control system. Each control system is under the responsible charge of an operator holding a valid certification equal to or greater than the classification of the control system. Organizations should require that all operating personnel making process control/system integrity decisions that affect potential risks be certified. Organizations should require a designated certified operator be present for each operating shift.

Internal Audits

Organizations should collect information and periodically evaluate the success of their security assessment techniques and other mitigation risk control activities. The organization should also evaluate the effectiveness of its management systems and processes in supporting sound security management decisions. Examples of items to review include the following:

- Current security and environmental regulations
- Examine items for relevancy and validity
- Compliance and infraction statistics
- Enforcement and management follow-up
- Budget and staffing for the personnel security program
- Training relevancy and currency
- Training requirements versus examination performance
- Data management system
- SVA results, accuracy, action items.

Keeping detailed records of security incidents help managers should be able to spot trends and assemble facts that lead to successful investigations. Some security managers use incident management software, which has graphing, charting, and search functions that can help bring an offense or loss pattern to light and identify issues of security concern. Incident data is only available for analysis if incidents are reported and recorded. Managers should establish several channels for incident reporting. For example, they may decide to make available the phone number and e-mail address of the person in charge of audits. Some companies have set up anonymous employee hot lines to encourage employees to report suspicions. It may also be useful to make it obligatory for employees to report security incidents. Then the managers can regularly analyze transaction histories, looking for variances from the norm. In addition to checking users' authorizations, managers can pay attention to unusual times, frequencies, and lengths of access. Organizations should consider auditing their personnel security program within 12 months of the effective date of implementation and thereafter to ensure that the requirements of these guidelines are satisfied.

External Audits

Organizations should require personnel security programs that will include ongoing outside involvement in the revision and operations of the personnel security program. A stakeholder board or advisory committee is strongly recommended. Examples of stakeholders are:

- Operators

- Environmental/public health groups
- Police/security groups
- The general public
- Primary vendors and subcontractors
- Process control technical assistance providers
- Organization managers
- Trainers.

Organizations should consider external reviews at least every few years.

Contractor/Vendor Audits

Organizations that accept the personnel security program of a contractor or vendor should have access to records and should consider auditing contractor or vendor programs every 12 months to ensure the requirements of these guidelines are satisfied. Organizations should be required to retain the responsibility for the effectiveness of contractor's and/or vendor's personnel security programs to include findings, recommendations, and corrective actions.

Enforcement

Organizations should have the ability to suspend operator certifications or take other appropriate enforcement action for operator misconduct. Examples of an individual's misconduct include:

- Fraud
- Falsification of application
- Falsification of operating records
- Gross negligence in operation
- Incompetence
- Failure to use reasonable care or judgment in the performance of assigned job duties
- A pattern of security infractions.

Emergency Plan

Organization's emergency plans should require training of key participants to ensure they have the skills and knowledge to effectively carry out those plans. A training and orientation program for key responders should be developed and periodically reviewed. Periodic exercises should include scenarios that include first responders from law enforcement, fire, and state authorities when appropriate. At the conclusion of all exercises, a comprehensive "lessons learned" critique should be conducted, and results should be incorporated into the emergency plans. Additionally, the exercise "lessons-learned" should be used as a basis for future training and orientation sessions.

Each organization should develop a means to advise and communicate to operator personnel and others as warranted by the security condition. Organizations should consider a means of establishing

emergency communications and contact information with appropriate agencies. Consider redundant emergency communications in both the hardware and the means for contacting agencies.

Control System Access

Control system areas should have personnel gates and/or turnstiles with electronic or biometric access control systems that record ingress and egress to physically secure control system areas such as:

- Motor control centers
- Rack rooms
- Server rooms
- Telecommunications rooms
- Control system rooms.

Organizations should control access to system areas using physical controls such as:

- Sign in logs
- Photo ID badges
- Key cards and/or number pads
- A close-circuit television system.

Organizations should also consider cyber security measures such as:

- Firewalls with effective configurations
- Virus protection with current updates
- DMZs to isolate business networks from operations
- Intrusion detection systems
- Encryption modules.

Follow the principles of “least access,” “need to know,” and “separation of functions,” and closely control the process of granting user authorizations, rather than allowing access by rank or precedent. Allow only authorized personnel to have physical access to central computer rooms and supervise any visitors.

Identification and authentication

Organizations should require use of rotating strong passwords or multi-factor authentication—include something “you know” (for example: passwords, destination IP address, and/or telephone number), something “you have” (for example: token, digital certificate), something “you are” (for example: biometrics) for access to the control room.

4. CONCLUSION

Conclusion

- Recruiting and screening trustworthy, capable, and safe individuals to secure control systems is vital.
- These personnel security concepts are broadly applicable.
- These personnel security guidelines are general; specific personnel security programs should be based on facility size, location, type, and existing security measures.
- Organizations should recognize and respond to the responsibility to protect their workers, communities, and supply/distribution networks through a variety of security based standards and procedures.

The concepts presented in this document are broadly applicable to control system personnel security and provide the starting point for developing personnel security guidance. This security guidance is, by necessity, general in nature. Individual organizations, working cooperatively with local officials, are best suited for conducting more detailed assessments of their own organizations and determining how best to protect their assets. This is because both potential threats and appropriate security measures vary significantly based on size, location, facility type and existing security measures already in place. Recognizing the vital importance of recruiting and screening trustworthy, capable, and safe individuals to secure an organization's control systems, a proactive and well-defined personnel security program is a top priority. From developing reliable and secure personnel security programs to protecting control system access and infrastructure to training with local emergency response teams, organizations should recognize and respond to the responsibility to protect their workers, communities, and supply/distribution networks through a variety of security based standards and procedures.

Since September 11th, many organizations have already reevaluated their control systems personnel security programs and voluntarily taken actions to improve personnel security programs as appropriate, based on the size, geographic location, potential risk to workers and the surrounding communities, and potential risk of attacks. To help organizations evaluate and respond appropriately to their potential and real security threats, the DHS has evaluated selected security program guidance to prepare this personnel security guidance. This guidance builds on the existing solid foundations of trustworthiness, capability, and operationally safe practices, which relate to organizational design and safety, environmental protection, emergency response, and protection from vandalism.

5. REFERENCES

"Blackout Was Preventable, Probe Finds," (www.cnn.com/2004/US/04/05/blackout.report/index.html), May 18, 2004

Parks, Bill, 2003, "Transforming the Grid to Revolutionize Electric Power in North America," *U.S. Department of Energy, Edison Electric Institute's Fall 2003 Transmission, Distribution and Metering Conference, October 13, 2003.*

DOE

DOE M 472.1-1B, *DOE Personnel Security Program Manual*, July, 2001.

DOE O 472.1C, *Personnel Security Activities*, March, 2003.

NRC

10 CFR 73.56, *Personnel access authorization requirements for nuclear power plants*

10CFR 73.57, *Requirements for criminal history checks of individuals granted unescorted access to a nuclear power facility or access to Safeguards Information by power reactor licensees*.

API

Security Guidelines for the Petroleum Industry (Second Edition)

ISA

ISA-TR99.00.01-2004, *Security Technologies for Manufacturing and Control Systems*

ISA-TR99.00.02-2004, *Integrating Electronic Security into the Manufacturing and Control Systems Environment.*

ISA Certified Control System Technician (CCST) Program (www.isa.org)

EPA

Federal Register SDWA Section 1419, *Guidelines for the certification and re-certification of operators of community and non-transient, non-community public water systems.*

CIDX

Site Security Guidelines for the U.S. Chemical Industry (American Chemistry Council Chlorine Institute, Inc. and Synthetic Organic Chemical Manufacturers Association)

Guidance for Addressing Cybersecurity in the Chemical Sector, Version 2.0, Preliminary Draft.

NERC

Security Guidelines for the Electricity Sector (Version 1.0).

Appendix A

Organization Criteria Comparison

Appendix A

Organization Criteria Comparison

Table A-1. Organization criteria comparison.

Concepts	Criteria	ISA	NRC	DOE	EPA	NERC	API	CIDX
Trustworthiness	Background Investigation	Employment verification forms signed by former employer, true identity, education history, credit history, criminal history, motor vehicle or drivers license history, and military history.	Employment history, verify true identity by fingerprints, education history, credit history, criminal history, motor vehicle or drivers license history, and military history.	Employment history, verify true identity, education history, credit history, criminal history, motor vehicle or drivers license history, and military history.	Employment history, verify true identity, education history, credit history, criminal history, motor vehicle or drivers license history, and military history.	Employment history, verify true identity, education history, credit history, criminal history, motor vehicle or drivers license history, and military history.	Employment history, verify true identity, education history, credit history, criminal history, motor vehicle or drivers license history, and military history.	Employment history, verify true identity, education history, credit history, criminal history, motor vehicle or drivers license history, and military history.
	Physical Qualifications	NA	Operators shall successfully pass a physical examination, designed to measure the individual's physical ability to perform assigned job duties, administered by a licensed physician.	Operators shall successfully pass a physical examination, designed to measure the individual's physical ability to perform assigned job duties, administered by a licensed physician	NA	NA	NA	NA
	Mental Qualifications	NA	Demonstrate through tests that the operator can exercise good judgment, implement instructions, assimilate assigned tasks, and communicate.	NA	NA	NA	NA	NA
	Psychological Assessment	NA	Evaluate through tests the possible psychological characteristics which may have a bearing on trustworthiness, emotional instability, and reliability.	NA	NA	NA	NA	NA
	Behavioral Observation	NA	Designed to detect individual behavioral changes that could lead to detrimental acts. No established history of alcoholism or drug addiction.	NA	NA	NA	NA	NA
	Voluntary Assessment	NA	Gives an individual an opportunity to report any information concerning authorization to perform job duties.	Gives an individual an opportunity to report any information concerning authorization to perform job duties.	NA	NA	NA	NA

Table A-1. (continued).

Concepts	Criteria	ISA	NRC	DOE	EPA	NERC	API	CIDX
Trustworthiness	Continuing Assessment	NA	Continuing observation for indications of trustworthiness, emotional stability, and reliability.	Continuing observation for indications of trustworthiness, emotional stability, and reliability.	Continuing observation for indications of trustworthiness, emotional stability, and reliability.	Continuing observation for indications of trustworthiness, emotional stability, and reliability.	Continuing observation for indications of trustworthiness, emotional stability, and reliability.	Continuing observation for indications of trustworthiness, emotional stability, and reliability.
Capability	Education and Experience	Industry experience	High school diploma or GED or equivalent performance examination, and industry experience.	High school diploma or GED or equivalent performance examination, and industry experience.	High school diploma or GED or equivalent performance examination, and industry experience.	High school diploma or GED or equivalent performance examination, and industry experience.	High school diploma or GED or equivalent performance examination, and industry experience.	High school diploma or GED or equivalent performance examination, and industry experience.
	Training	Control theory, analog and digital electronics, microprocessors and computers, operation and maintenance of particular lines of field instrumentation, pipe fitting, and electrical fundamentals	Each operator requires training as identified by the organization.	Each operator requires training as identified by the organization.	Each operator requires training as identified by the organization.	Each operator requires training as identified by the organization.	Each operator requires training as identified by the organization.	Each operator requires training as identified by the organization.
	Security Awareness	NA	Ongoing employee awareness sessions and training	Ongoing employee awareness sessions and training	Ongoing employee awareness sessions and training	Ongoing employee awareness sessions and training	Ongoing employee awareness sessions and training	Ongoing employee awareness sessions and training
	Ongoing Training	Organizations remain current with changes in technology.	Organizations remain current with changes in technology.	Organizations remain current with changes in technology.	Organizations remain current with changes in technology.	Organizations remain current with changes in technology.	Organizations remain current with changes in technology.	Organizations remain current with changes in technology.
	Certification Exams	Certification is based on exams with passing grades.	Certification is based on exams with passing grades.	Certification is based on exams with passing grades	Certification is based on exams with passing grades.	Certification is based on exams with passing grades.	Certification is based on exams with passing grades.	Certification is based on exams with passing grades.
	Equipment Training	Uses equipment that measures and controls level, temperature, pressure, flow, force, power, position, motion, physical properties, and chemical composition.	Uses equipment that measures and controls level, temperature, pressure, flow, force, power, position, motion, physical properties, and chemical composition.	Uses equipment that measures and controls level, temperature, pressure, flow, force, power, position, motion, physical properties, and chemical composition.	Uses equipment that measures and controls level, temperature, pressure, flow, force, power, position, motion, physical properties, and chemical composition.	Uses equipment that measures and controls level, temperature, pressure, flow, force, power, position, motion, physical properties, and chemical composition.	Uses equipment that measures and controls level, temperature, pressure, flow, force, power, position, motion, physical properties, and chemical composition.	Uses equipment that measures and controls level, temperature, pressure, flow, force, power, position, motion, physical properties, and chemical composition.

Table A-1. (continued).

Concepts	Criteria	ISA	NRC	DOE	EPA	NERC	API	CIDX
Secure Environment	Vulnerability and Risk Assessment	NA	Control systems must be classified based indicators of potential health, security, destruction, and infrastructure risk, which includes complexity and size.	Control systems must be classified based indicators of potential health, security, destruction, and infrastructure risk, which includes complexity and size.	Control systems must be classified based indicators of potential health, security, destruction, and infrastructure risk, which includes complexity and size.	Control systems must be classified based indicators of potential health, security, destruction, and infrastructure risk, which includes complexity and size.	Control systems must be classified based indicators of potential health, security, destruction, and infrastructure risk, which includes complexity and size.	Control systems must be classified based indicators of potential health, security, destruction, and infrastructure risk, which includes complexity and size.
	Hierarchy	Three certification levels	Operators are certified equal to or greater than the classification of the control system.	Operators are certified equal to or greater than the classification of the control system.	Operators are certified equal to or greater than the classification of the control system.	Operators are certified equal to or greater than the classification of the control system.	Operators are certified equal to or greater than the classification of the control system.	Operators are certified equal to or greater than the classification of the control system.
	Internal Audits	NA	Every 2 years	Every 2 years	Every 3 years	Every 2 years	Suggested	Every 3 years
	External Audits	NA	NA	NA	Every 5 years	Suggested	Suggested	Suggested
	Contractor/ Vendor Audits	NA	Every 12 months	Every 12 months	Suggested	Suggested	Suggested	Suggested
	Enforcement	Ability to suspend operator certifications or take other appropriate enforcement action for operator misconduct.	Ability to suspend operator certifications or take other appropriate enforcement action for operator misconduct.	Ability to suspend operator certifications or take other appropriate enforcement action for operator misconduct.	Ability to suspend operator certifications or take other appropriate enforcement action for operator misconduct.	Ability to suspend operator certifications or take other appropriate enforcement action for operator misconduct.	Ability to suspend operator certifications or take other appropriate enforcement action for operator misconduct.	Ability to suspend operator certifications or take other appropriate enforcement action for operator misconduct.
	Emergency Plan	NA	Industry ensures that operators have the skills and knowledge to effectively carry out emergency actions.	Industry ensures that operators have the skills and knowledge to effectively carry out emergency actions.	Industry ensures that operators have the skills and knowledge to effectively carry out emergency actions.	Industry ensures that operators have the skills and knowledge to effectively carry out emergency actions.	Industry ensures that operators have the skills and knowledge to effectively carry out emergency actions.	Industry ensures that operators have the skills and knowledge to effectively carry out emergency actions.
	Control System Access	NA	Sign in logs, photo ID badges, key cards and/or number pads, close-circuit television system, firewalls, virus protection, and intrusion detection systems	Sign in logs, photo ID badges, key cards and/or number pads, close-circuit television system, firewalls, virus protection, and intrusion detection systems	Sign in logs, photo ID badges, key cards and/or number pads, close-circuit television system, firewalls, virus protection, and intrusion detection systems	Sign in logs, photo ID badges, key cards and/or number pads, close-circuit television system, firewalls, virus protection, and intrusion detection systems	Sign in logs, photo ID badges, key cards and/or number pads, close-circuit television system, firewalls, virus protection, and intrusion detection systems	Sign in logs, photo ID badges, key cards and/or number pads, close-circuit television system, firewalls, virus protection, and intrusion detection systems
	Communication	NA	Establishing emergency communications and contact information with appropriate agencies.	Establishing emergency communications and contact information with appropriate agencies.	Establishing emergency communications and contact information with appropriate agencies.	Establishing emergency communications and contact information with appropriate agencies.	Establishing emergency communications and contact information with appropriate agencies.	Establishing emergency communications and contact information with appropriate agencies.

Appendix B

News Article

Blackout was preventable, probe finds

Task force says 2003 outage not caused by terrorist attack

Tuesday, May 18, 2004 Posted: 11:21 PM EDT (0321 GMT)

(CNN) -- Last summer's power outage that plunged parts of eight states and a Canadian province into darkness could have been prevented and was not a terrorist or cyber attack, according to a final report released Monday by an investigative task force.

The task force's co-chairmen -- U.S. Energy Secretary Spencer Abraham and R. John Efford, Canadian minister of natural resources -- said the group would remain active for another year to push for its recommendations.

The blackout, which started on August 14, was the largest ever to hit the United States. It affected all or most of Ohio, Michigan, Pennsylvania, New York, New Jersey, Vermont, Massachusetts, Connecticut and Ontario province.

Power was restored to most localities, including New York City, by the end of the next day, but some places were without electricity for several days.

The task force especially focused on the need for mandatory reliability regulations in the United States and Canada, with government oversight and penalties for noncompliance.

The power industry now has voluntary requirements aimed at preventing blackouts. They are administered by the private North American Electric Reliability Council, which lacks the ability to hand down penalties.

Many reliability rules were ignored during the outages, the task force said.

"The report makes clear that this blackout could have been prevented and that immediate actions must be taken in both the United States and Canada to ensure that our electric system is more reliable," the chairmen said in a statement.

After the task force issued its interim report in November, subcommittee members continued to examine the possibility of terrorist instigators, the report said.

While acknowledging al Qaeda claims of responsibility, there was no proof of the group's involvement, it concluded.

As it did in its interim report, the task force largely blamed FirstEnergy Corp., based in Akron, Ohio, for the electrical failures on August 14, faulting the company's lack of communication, faulty equipment and inadequate training.

The task force said three power line failures in Ohio should have been contained by FirstEnergy operators.

As a result, the outage cascaded, eventually cutting off electricity to 50 million people.

"The FE operators received pertinent information [August 14] ... but did not recognize the emerging problems from the clues offered. This pertinent information included calls such as that from FE's eastern control center asking about possible line trips," the report said.

It took only seven minutes, the task force said, for interruptions on the high-voltage system to spread from the Cleveland-Akron area of Ohio across much of the northeast United States and Canada.

FirstEnergy admitted a few days after the power failures that it lost three of its own transmission lines and one it co-owns in the hour preceding the blackout. The company also said its computer alarm systems were not functioning.

The task force also noted that some of the power interruptions were due to trees interfering with power lines.

Task force recommendations include:

- Strengthening the institutional framework of the North American Electric Reliability Council and developing a funding mechanism for it to help ensure its independence from the companies it oversees.
- Addressing deficiencies at FirstEnergy by June 30.
- Improving training and certification requirements for operators, reliability coordinators and support staff.
- Increasing the network's physical and cyber security.

ACKNOWLEDGMENTS

Under direction from the Department of Homeland Security (DHS), this document was created by reviewing several organizations' personnel security guidance documents. All of these documents were provided for the express purpose of supporting the DHS in preparing this report, or are currently available on the Internet. Materials used in this report, including the Chemical Industry Data Exchange "Preliminary Draft Guidance for Addressing Cyber security in the Chemical Sector, Version 2.0," and the American Petroleum Institute "API Standard 1164, SCADA Security, First Edition," were developed in support of their memberships and are examples of industry taking the lead in protecting the critical infrastructure. We recognize that this work was privately funded, and the copyright protection covering these documents precludes extensive citation. Our thanks and recognition are offered to them for this support and their diligent efforts.