INL/EXT-05-00043

US-CERT Control Systems Security Center FY 2004 Program Summary

Robert E. Polk

April 2005

The INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance

INL/EXT-05-00043

US-CERT Control Systems Security Center
FY 2004 Program Summary

Robert E. Polk

April 2005

US-CERT Control Systems Security Center
Idaho Falls, Idaho 83415

Prepared for the
U.S. Department of Homeland Security
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

US-CERT Control Systems Security Center

FY 2004 Program Summary

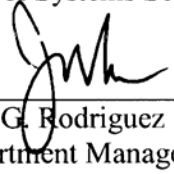
INL/EXT-05-00043

April 2005

Approved by:

Fred C. Cowart
Program Manger
Control Systems Security Center

4/22/05
Date



Julio G. Rodriguez
Department Manager
Critical Infrastructure Assurance

4/22/05
Date

ABSTRACT

In May 2004, the US-CERT Control Systems Security Center (CSSC) was established at Idaho National Laboratory to execute assessment activities to reduce the vulnerability of the nation's critical infrastructure control systems to terrorist attack. The CSSC implements a program to accomplish the five goals presented in the *US-CERT National Strategy for Control Systems Security.* This report summarizes the first year funding of startup activities and program achievements that took place in FY 2004 and early FY 2005.

This document was prepared for the US-CERT Control Systems Security Center of the National Cyber Security Division of the Department of Homeland Security (DHS). DHS has been tasked under the Homeland Security Act of 2002 to coordinate the overall national effort to enhance the protection of the national critical infrastructure. *Homeland Security Presidential Directive HSPD-7* directs federal departments to identify and prioritize the critical infrastructure and protect it from terrorist attack. The *US-CERT National Strategy for Control Systems Security* was prepared by the National Cyber Security Division to address the control system security component addressed in the *National Strategy to Secure Cyberspace* and the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. The *US-CERT National Strategy for Control Systems Security* identified five high-level strategic goals for improving cyber security of control systems.

CONTENTS

ACRONYMS

CSSC	Control Systems Security Center
DHS	Department of Homeland Security
DOE	Department of Energy
GAO	General Accounting Office
HSPD-7	Homeland Security Presidential Directive-7
INL	Idaho National Laboratory (formerly INEEL—Idaho National Engineering and Environmental Laboratory)
IORC	Information Operations and Research Center (cyber and control system test center at INL)
KEMA	Utility services company, including SCADA security
PSD	Protective Security Division
NCSD	National Cyber Security Division
PMP	Project Management Plan
SAV	Site assist visit
SCADA	Supervisory Control and Data Acquisition
SME	Subject matter expert
US-CERT	U.S. Computer Emergency Readiness Team
VA	Vulnerability assessment

FY 2004 Program Summary

1. INTRODUCTION

This document has been prepared for the US-CERT Control Systems Security Center of the National Cyber Security Division (NCSD) of the Department of Homeland Security (DHS) to provide a summary of FY 2004 activities that were accomplished for a new program initiative. This initiative was in response to its task under the Homeland Security Act of 2002 to coordinate the overall national effort to enhance the protection of the national critical infrastructure. *Homeland Security Presidential Directive HSPD-7* directs the federal departments to identify and prioritize the critical infrastructure and protect it from terrorist attack.

The *US-CERT National Strategy for Control Systems Security* (the "Strategy") was the first major task under the new program initiative. It was prepared by the NCSD to address the control system security component addressed in the *National Strategy to Secure Cyberspace* and the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. The Strategy incorporates the following five highly integrated goals to deal with the issues and problems associated with control systems security through the US-CERT Control Systems Center:

1. Facilitate the US-CERT capability to coordinate control system incident management, provide timely situational awareness information for control systems, and manage control system vulnerability and threat reduction activities.
2. Creation of a Control Systems Security Center that provides a proactive environment for vulnerability reduction and security testing.
3. Bridge industry and governmental efforts through participation in working groups, standards development bodies, and user conferences to build cooperative and trusted relationships and enhance control systems security efforts.
4. Develop control systems security awareness and create a self-sustaining security culture within the control systems community.
5. Make strategic recommendations as to the funding, development, and testing of next-generation secure control systems and security products.

To accomplish these goals, the NCSD established the US-CERT Control Systems Security Center (to be referred to as the CSSC)[a] Program at Idaho National Laboratory (INL)[b] in April 2004. The CSSC Program is the focal point for eliminating vulnerabilities associated with cyber security of control systems for critical infrastructure throughout the U.S. Efforts associated with this objective are coordinated through the CSSC Program and use nationally available

---

a. The Strategy recommended a Control Systems Security and Test Center, which became the initial program title; the title was subsequently changed to the Control System Security Center (CSSC).

b Idaho National Laboratory was renamed from the Idaho National Engineering and Environmental Laboratory (INEEL) on February 1, 2005. Documents generated by the CSSC prior to February 1 will have the previous Laboratory designation as the developer.

facilities, tools, capabilities, and expertise to identify and eliminate control system vulnerabilities. The mission of the CSSC Program is to secure the critical U.S. infrastructure by identifying, analyzing, and eliminating vulnerabilities associated with the control systems that govern these infrastructures.

1.1 CSSC Program Objectives

The FY-04 Program Objectives were:

- Develop a National Strategy for the protection of control systems.
- Stand up the CSSC Program including the assessment capability for control systems at INL.
- Provide support to the U.S. Computer Emergency Readiness Team (US-CERT) control system incident management capability by responding to emergencies related to control system cyber anomalies and/or attacks.
- Provide near-term vulnerability reduction.
- Provide an environment in which DHS can assist stakeholders in the national effort to secure critical infrastructure control systems.
- Provide system testing capabilities for users and vendors of control systems.
- Provide analytical capabilities to identify threats and risks, evaluate consequences and likelihoods, and recommend priorities for mitigative actions.
- Support DHS efforts to bridge industry and governmental security initiatives by participation in working groups, standards development bodies, and user conferences to build cooperative and trusted relationships and enhance control systems security efforts.
- Assist control system stakeholders in developing and implementing solutions, supporting control systems security awareness, and creating a self-sustaining security culture within the control systems community.

The CSSC Program was funded $10M in FY 2004 to startup and provide immediate benefits and accomplishments directed toward vulnerability reduction and meeting the goals within the Strategy. The CSSC Program accomplishments for FY 2004 are presented in the following section.

2. CSSC ACCOMPLISHMENTS AND CAPABILITIES

The activities and status from April 2004 through January 2005 of the CSSC Program are summarized in the following table. Abstracts of deliverable product reports are provided in Appendix A.

Title	Description	Status[a]	Comments/Next Step
Functional Control Systems Security Center Program	Organized and started up the program. Set up leadership teams with three other DOE Laboratories. Initiated and completed various short-term vulnerability reduction tasks.	Operational 08/04	Manage and operate the CSSC.
US-CERT National Strategy (Draft)	Developed for control systems security. DHS summarized it and released it to the Government Accountability Office (GAO).	Complete DHS released to GAO on 8/04	Update planned to be completed in FY-05. Original served as a scoping effort for the development of the "NCSD/US-CERT Strategy for Control Systems Security." The Strategy provided the basis for the program development.
Personnel Security Guidelines	Industry requested that DHS compile personnel security guidelines for industry. Analyzed the approach used by seven major industries and organizations. A recommendation was based on this analysis.	Complete	Could be revised to incorporate industry feedback. Not all recommendations can be realistically followed within industry. Serves as a data point for some of the governance issues that the security framework will encompass.
VA Best Practices	Best practices and methods for vulnerability assessments (VAs) of SCADA systems were shared by the six DOE National Laboratories, and a consensus for the need of a standard methodology/process for VAs of private and government sectors is being developed. This standard process will be used by all six Laboratories in conducting and executing VA assessments. This activity leveraged the best experience in cyber assessment that spans most of the critical infrastructure sectors.	In progress, estimated completion 05/05	Coordinate any planned or requested assessments with appropriate DOE Laboratory skill set.

a Status includes the approximate cost and duration of the task in months.

Title	Description	Status[a]	Comments/Next Step
"Gold Disk" Testing and Evaluation	Develop implementation recommendations for particular systems and/or combinations of products and components. These recommendations will define the minimum level of control system security that would be required to protect these systems from known potential intrusion or cyber exploitation pathways.	Ongoing	A cooperative code-base analysis will be completed with the manufacturer and specific recommendations will be developed for the underlying protocol, operating system, and hardware support necessary for the application to function. The recommendations will be developed against the security requirements and assurance levels defined within the control systems security framework.
Workshops	Hosted an Industry Involvement Workshop, June 2004, to solicit input for the goals and missions of the CSSC Program. Hosted a National Laboratory Workshop, August 2004, to define potential contributions and capabilities.	Complete	Hold additional workshops in FY-05. Include threat briefings, demonstrations, and recommendations.
Industry Advisory Group	Set up mechanism to obtain input from key industry sectors.	Planning stage	On hold. May integrate with other DHS critical infrastructure outreach programs.
US-CERT Support Team	Developed a quick response cell at INL to support US-CERT in handling control systems-specific incidents/ events. Also recommended improvements in the US-CERT process to help identify control systems events. Developed initial vulnerability analysis and incident response workflow and methodology. Have already responded to frequent urgent requests.	Operational (partial) 07/04	Original intent was 24/7 support. Funding was cut and INL is only providing occasional support as requested by DHS.
Outreach Implementation & Training	Identify industrial clients and parties interested in working with the CSSC. Develop and conduct training sessions.	Completed initial activities	Continue and expand outreach and coordination with industry.
Control Systems Security Standards	Prepared (jointly with DOE funding) three reports that evaluated control systems security standards: INEEL/EXT-04-02428—A Comparison of Electrical Sector Cyber Security Standards INEEL/EXT-04-02462—A Comparison of Cyber Security Standards Developed by the Oil and Gas Segment INEEL/EXT -04-02425—Standards – Status and Path Forward	Complete	Standards coordination support is an ongoing effort in FY-05. Recommended security requirements are being developed by the program and will be compared against existing and planned standards (gap analysis).

Title	Description	Status[a]	Comments/Next Step
Expanded INL Test Facility (IORC)	Set up seven SCADA test bays and a classified cyber test area. Constructed new entryway, reception area, turnaround area, conference rooms, and control/training room. Procured and set up control systems components to establish representative control networks.	Operational	Additional test beds planned in FY-05. Also, installation of additional input/output (I/O) for enhanced testing (plug and play components) is planned in FY-05.
Chemical Process Control System Test Bed	Demonstration Facility. Fully operational chemical processing facility with a Virtual Private Network (VPN) to IORC, suitable for conducting cyber control tests.	Operational	Will use to develop demonstration of chemical spill and for incident response/mitigation.
Open Source Vulnerability Assessments	Conducted an open-source assessment of four critical infrastructure sectors to determine if open public information was available, and if the information could be gathered and compiled to develop threat and attack scenarios.	Complete	Has led to generation of FBI bulletins and advisories regarding the risk exposure that open-source information presents to industry.
Interview Assessment Template	Developed a comprehensive assessment template for field data collection on SCADA systems within critical infrastructures. The template leveraged the process used within the Site Assist Visit (SAV) program conducted by the Protective Service Division (PSD) with an extended level of detail to support vulnerability assessment test planning and risk analysis.	Complete	Use of this template by the CSSC in collaboration with PSD is anticipated for critical infrastructure assessments that have a significant SCADA element.
Self-Assessment Tool	Web-based toolkit that will walk owners and operators of critical infrastructure control systems through a self-assessment questionnaire designed to allow individual evaluation of their current level of cyber security assurance, as defined within the control systems security framework.	Planning stage	FY-05 activity
Alyeska Review	Trans Alaska Pipeline Control System Upgrade Cyber Security Assessment (INEEL/EXT 04-02426)—At the request of Alyeska Inc., the Center reviewed and performed testing on new system design and installation.	Complete	
Metso Test Bed	Complete Distributed Control System (DCS) test system with direct connectivity to INL nuclear test area. Connected to test range.	Operational	Will be utilized for component testing against control systems.

Title	Description	Status[a]	Comments/Next Step
Citect Test Bed	Complete SCADA test system with direct connectivity to INL power grid.	Operational	Replica will be installed in IORC with direct connectivity to a substation.
Evaluate August 2003 Power Blackout	Review the Northeast Power Blackout Report and compare the direction and strategy of the Control System Security Program with the Report recommendations.	Submitted draft report	
I/O upgrade	The Input/Output (I/O) upgrade to the Test Bed within the IORC facility at INL will provide for in-depth assessments of control systems in a true-to-life environment through the expansion of I/O and system capabilities.	Completed conceptual design	Installation planned for FY-05.
Site Assist Visit Report Reviews	Reviewed prior site assessment reports to assess the methodologies and data for possible use. Results published in report INEEL/EXT-04-02369, "Assist Visit Report Reviews."	Complete	
Control Systems Security Framework Design	Establishes the DHS/NCSD baseline for control systems security. Develop and implement a framework in FY-05 for control systems cyber-security (e.g., systems definitions, protection profiles, assurance levels, security program).	Completed conceptual design	Complete design and develop self assessment tool for industry.
Gross Consequence Matrix and Impact Analysis	Created a prioritized list of specific sites from the National Asset Database where control systems could have an effect on initiating or mitigating a negative consequence due to failure or terrorist activity.	Complete	The Consequence Matrix will be refined in FY-05 using the new risk analysis methodology.
Control Systems Risk/Decision Analysis Tools	Developed a methodology to calculate risk (i.e., annual expected loss as a result of a successful attack on a cyber system).	Report describing methodology for risk and decision analysis was completed 2/05.	Additional tools and data population will be accomplished in FY-05. Support testing and various analysis tasks as requested.

3. PROGRAM PERFORMANCE

3.1 Budget – Schedule

Task Descriptions		Costs
Task 1 - Draft National Strategy		**$654,360**
Task 2 - Operable Control System Security Center		**$4,244,790**
Center Start-up, Training and CERT Operations	$1,433,742	
Security Center Operations	$754,407	
Security Center Facility Mods and Equipment	$2,056,641	
Task 3 - Vulnerability Reduction		**$3,869,362**
Near-Term Vulnerability Reduction Tasks	$800,651	
Mid-Term Vulnerability Reduction Tasks	$3,068,711	
Program Administration		**$1,231,488**
Program Management, NCSD Support, Planning	$1,037,097	
Database Development w/ FY-04 Carryover	$194,391	
	Total FY-04 Costs	**$10,000,000**

Figure 1. Summary of FY-04 CSSC Expenditures.

The FY-04 funding total of $10M was received on May 3, 2004. Program activities were initiated with the development of a Start-up Execution Plan, which established budgets for the program tasks. Figure 1 above shows the actual expenditures at the summary levels tasks. The FY-05 funding for the program was received in late January 2005 and FY-04 funding was, therefore, carried forward as various ongoing activities continued in the first quarter of FY-05. All FY-04 scope was completed within the $10M funding limit for FY-04.

All commitments for major deliverables defined in the program Startup Execution Plan were completed within the overall budget and by the established date. The cost for upgrades to the Idaho Operations Research Center (IORC) was, however, higher than estimated. This is due to the extra effort to meet a formally announced opening ceremony and increased costs associated with workarounds for certain materials that were not available to meet the scheduled opening day. Also, unanticipated minor upgrades to the entire IORC facility were needed and contributed to the higher than estimated expenses in the facility upgrade budget. These additional expenses were covered by underruns in other budget accounts.

3.2 Issues

The most significant issue affecting conduct of program execution beyond the initial startup was the uncertainty and associated delay of an FY-05 budget appropriation. The CSSC

implemented a FY-04 Carryover Working Budget to control the work being performed using the remaining FY-04 funding. The delay in determining the amount and timing of the FY-05 funding resulted in significant rework of priorities and tasking into January 2005.

4. SUMMARY AND CONCLUSION

Startup of the CSSC Program and the initial vulnerability reduction activities were successfully executed. Significant visibility of the issues with control systems vulnerability was provided to private and government sectors by the activities of the CSSC. Integrated testing capability for large computer-based control systems was developed and applied to private-sector vulnerability identification and reduction. The development of control systems security risk and consequence models has begun to meet a gap in methodology and analysis for cyber control systems. The CSSC has a role to fulfill the DHS mission for prevention, detection, and mitigation of consequences from terrorist cyber attack on control systems for the national critical infrastructure assets. In addition, the CSSC provides a valuable contribution to meeting the goals and objectives of the Interim National Infrastructure Protection Plan. The CSSC startup phase has concluded with advancement of the mission objectives to be worked in FY 2005.

The FY 2005 effort consists of four major initiatives: control systems risk and impact analysis, cyber testing of control systems representative of non-energy sectors, improvement of standards relevant to control systems across all sectors, and development of a comprehensive security framework for control systems security. The security framework will strive to present controls systems vulnerability reduction methodology and tools that owners/operators and vendors can use to meet specific objectives and requirements for more secure control systems.

The FY 2005 Annual Work Plan was approved by DHS NCSD on January 28, 2005.

Appendix A

Abstracts from Key Program Deliverables

Appendix A

Abstracts from Key Program Deliverables

Program Execution Plan (INEEL/EXT-04-02149)

The National Cyber Security Division (NCSD) of the Department of Homeland Security (DHS) is establishing a Control Systems Security Center (CSSC) Program. A critical component of the program is an operating center at Idaho National Laboratory (INL) in Idaho Falls (herein referred to as "the Center"). The Center includes facilities, tools, capabilities, and expertise to assist in vulnerability research and mitigation. The purpose of the Center is to assist NCSD in identifying and reducing control system-related vulnerabilities critical to U.S. domestic security. Control systems underlie a significant part of the nation's critical infrastructure and are vulnerable to attacks by U.S. adversaries that could result in loss of life, severe economic impact, or both.

National Strategy for Control Systems Security

Our nation clearly depends on the continuous and effective performance of a vast infrastructure to sustain our modern way of life. This infrastructure is comprised of vital physical, human, and computer-based systems and assets that, if incapacitated or destroyed, would have a debilitating impact on national security, economic security, public health and safety, the environment, or any reasonable combination thereof. Control systems are integral components of our critical infrastructure, many of which perform the vital tasks of monitoring and controlling sensitive processes and functions. DHS has been tasked under the *Homeland Security Act of 2002* to coordinate the overall national effort to enhance the protection of the national critical infrastructure.

This strategy document flows naturally from the mission of "Protecting Critical Infrastructure and Key Assets," identified in the *National Strategy for Homeland Security.* It addresses the physical, cyber, and communications vulnerabilities associated with our nation's infrastructure. Furthermore, Congress requested an assessment of the potential security vulnerabilities, significant risks, and key challenges of protecting these control systems against malicious attack. In response, the General Accountability Office (GAO) recommended that DHS develop and implement a strategy for coordinating various ongoing efforts within the private sector and other government agencies to improve control system security. The DHS has already initiated programs to improve control system security consistent with the strategy presented in this document.

The individual goals and objectives to secure control systems as set forth in this national strategy are reflections of what industry says it needs to protect its customers and investors as well as the public. In accomplishing greater security for critical infrastructure, the actions will also protect and strengthen public confidence and valued assets. As tragic as the events of 9/11 were, the cascade of events leading to loss of public confidence have impacted many more people due to loss of jobs and value in the economy. This strategy will be updated and reissued annually to reflect the progress and highlight the current initiatives for the concerned community of control system users and vendors.

Program Managemen Plan (INEEL/EXT-04-02249)

This document establishes the Program Management Plan (PMP) for the CSSC at INL. The purpose of the PMP is to define the overall program and the elements of the program.

The PMP describes how the CSSC performs the following functions:

- Align management systems, resources, and priorities for operating the CSSC as the nation's coordinating function for identifying, reducing, and eliminating vulnerabilities associated with control systems in the critical infrastructure
- Integrate and focus all CSSC work and deliverables under an integrated management structure with a single point of control
- Foster relationships between other agencies, national laboratories, industry, universities, and other participants, and foster synergy among participants in integrating CSSC work.

Achieving the goals identified above will help ensure the nation's critical infrastructure is moving towards a more secure and reliable state.

Control System Personnel Security Guidelines (INEEL/EXT-04-02264)

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 U.S. 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.

Site Assist Visit Process Template (INEEL/EXT-04-02364)

This document was prepared by the CSSC as part of the Near-term Task 3-3, SAV Process Template/Report. The purpose of the task was to prepare an assessment guide to help gather information from the field at critical infrastructure sites. This task supports Goal 1 of the *US-CERT National Strategy for Control Systems Security* which, in part, seeks to, "develop comprehensive vulnerability assessment and risk analysis methodologies."

The desired information provides sufficient detail to allow modeling of the system architecture for vulnerability assessment, testing, and mitigation. The guide, in the form of a template, is based on previous templates used within the DHS Site Assist Visit (SAV) program, and is augmented by experts in cyber vulnerability assessment and process control systems. We anticipate that this guide will be used by the CSSC in future assessments with the potential for augmenting the SAV program within the DHS Protective Security Division. CenterPoint Energy (Houston, Texas) reviewed the template and provided valuable comments that can serve as possible enhancements for future template revisions.

Site Assist Visit Report Reviews (INEEL/EXT-04-02369)

This document was prepared by the CSSC as part of the Near-term Task 3-5, SAV Database Evaluation Report. The purpose of the task was to review prior site assessment reports to assess the methodologies and data for possible use in CSSC analysis and testing activities. This task supports Goal 2 of the *US-CERT National Strategy for Control Systems Security* which is to, "provide a practical testing and evaluation capability in a technical center to evaluate existing and next-generation systems, and work with the users and vendors to resolve identified vulnerabilities."

DHS's Protective Security Division has conducted site assessments on facilities representing various infrastructure segments since March of 2003. Prior to DHS, the Department of Energy's Office of Energy Assurance conducted assessments in 2002 and 2003. These assessments were conducted to provide information that defined the critical assets, impact, and vulnerabilities of these sites to terrorist attack—primarily physical. Reports were generated to document these assessments and provided a resource in reviewing the assessment methodology and data for possible use in CSSC analysis and testing activities. Approximately 100 reports were reviewed. The utility of the information on a majority of the reports was insufficient for control system applications since the assessments were primarily focused on physical attacks. The SAV program provides a unique opportunity to get specific field data, but needs to be augmented by additional detail for those sites of particular interest to DHS NCSD and the CSSC.

Control Systems Security Program Survey (INEEL/EXT-04-02131)

This evaluation accomplishes a goal set forth in the DHS draft *US-CERT National Strategy for Control Systems Security*. INL was tasked to identify control system security-related programs at national laboratories, academic institutions, and agencies; evaluate their respective value to the CSSC; and recommend how selected program activities could be leveraged to reduce control system vulnerabilities. The focus was on domestic public sector programs because they could be more readily leveraged than activities in the private and international sectors. This report documents the results of that task, which consisted of establishing program evaluation criteria, identifying potential programs, gathering germane information about those programs, assessing that information, and formulating recommendations on how

the CSSC can leverage selected activities to accomplish its mission. This report expands on the interim evaluation published in August, which is already being used by the CSSC, to include a list of control system security-related capabilities within the national laboratories and a cursory gap analysis of control system security-related needs identified by participants in the development of the *Draft National Strategy for Control System Security*, consistent with requests received while preparing this update. Future evaluations will be part of an ongoing, iterative process of the CSSC infrastructure via outreach activities, and may eventually expand to include international and private sector control system security programs. This report is based on information available as of the publication date; it is not intended to be comprehensive of all programs, institutions, capabilities, etc.

Gross Consequence Matrix (INEEL/EXT-04-02156)

DHS developed the Process Control System (PCS) Gross Consequence Matrix that identifies and lists critical infrastructure elements such as refineries, chemical plants, electrical substations, and transportation facilities, prioritized by the probable consequences of control system sabotage. DHS tasked INL with populating the matrix with selected sites from the National Asset Database (NADB) to develop and apply a rough order of magnitude prioritization scheme based on consequence and relative contribution of control systems at a specific site.

INL assessed four sectors: refineries, chemical plants, electrical substations, and transportation, focusing specifically on Consequence of Attack (COA)/Consequence of Loss (COL) ranking. The level of control system use and degree of control system integration were considered in the evaluation. Weighting factors for impact to the surrounding population, effect on the local economy, and effect on the nationwide economy were used to prioritize the four sectors. The result is a prioritized list of specific sites on the NADB in which control systems may have an effect on prevention, initiation, or mitigation of a negative consequence due to failure or terrorist activity. The updated prioritized list in the four sectors is contained in classified Appendix D of the Gross Consequence Matrix, under separate cover. DHS may use this list and method to select sites for further study of the potential for cyber attack on complex control systems in critical infrastructures.

Risk Analysis Status Report CSSTC (INEEL/EXT-04-02378)

This report describes the status of work performed during August and September 2004 in support of the Analysis Function and presents the basis of a generic model and an approach to calculate quantitative values of risk in terms of defenders, attackers, system description, attack modes, threat, vulnerability, and worker and public health economic consequences. The thrust of the model development is to maximize the utilization of existing data for calculating risk values. At a minimum, the model will incorporate cyber technology and ingenuity, operable system descriptions, economic models, human factors and human reliability models, probabilistic risk analysis, uncertainty analysis, and graphical information systems. The model is scheduled for completion during the first part of FY 2005.

Standards—Status and Path Forward (INEEL/EXT-04-02425)

Cyber Security Standards will guide the development and implementation of control systems. The need for control systems security has grown significantly during the last few years due to the openness of systems, external connectivity, and an increased number of intrusions. This report presents an overview of cyber security standards and related documents and proposes means to use the standards process to

increase the level of security of critical infrastructure sectors by influencing selected standards through direct participation, education, and subcontracting of knowledgeable resources.

Trans Alaska Pipeline Control System Upgrade Cyber Security Assessment (INEEL/EXT-04-02426)

The Alyeska Pipeline Service Company is upgrading the control system for the Trans Alaska Pipeline System (TAPS). The upgrade will involve the installation of a new control system to replace the existing supervisory control and data acquisition (SCADA) system.

The objective of this document is to provide a preliminary cyber security assessment of the Alyeska Pipeline Service Company TAPS CSU, based on the document *Alyeska Network Plan for the SCADA Host/Historian Replacement Project*, release revision D, April 29, 2004. This assessment is being performed by the INL.

A Comparison of Electrical Sector Cyber Security Standards and Guidelines (INEEL/EXT-04-02428)

This paper presents a review and comparison (commonality and differences) of five security standards in the electrical distribution and control area. The comparison identifies security areas that are covered by each standard and reveals where the standards differ in emphasis. By identifying differences in standards the user can evaluate which standards best meet their needs. For this paper, only the standards applicable to the electrical segment were reviewed.

A Comparison of Cyber Security Standards Developed by the Oil and Gas Segment (INEEL/EXT-04-02462)

This report presents a review and comparison (commonality and differences) of two oil and gas segment cyber security standards and an internationally recognized information security standard. The comparison identifies security areas that are covered by each standard and reveals where the standards differ in emphasis. By identifying differences in the standards the user can evaluate which standard best meets their needs. For this report, only standards applicable to the oil and gas segment were reviewed.

Comparison of CSSC Activities Against Recommendations of the Final Report on the August 14, 2003 Northeast Power Blackout

The NCSD of DHS is working toward national-level coordination between government and industry to reduce vulnerabilities and respond to threats associated with the physical and cyber aspects of control systems in critical infrastructures, such as the North American power grid. In support of this goal, DHS requested that the CSSC at INL evaluate the 46 recommendations listed in the Blackout Report against the CSSC Program Management Plan mission and elements, as well as the five goals identified in the *Draft National Strategy for Control System Security*. The purpose of this evaluation is to identify specific areas where the task force recommendations should be supported through the CSSC, and to locate possible gaps or overlaps with planned CSSC functions.

Because the CSSC has only recently been established, it has not engaged in any specific power-grid related control system security projects that directly conflict or overlap the expected activities of the North American Electric Reliability Council, Federal Energy Regulatory Commission, Control Areas,

Reliability Coordinators, Grid Operators, Regional Transmission Organizations, Independent System Operators and/or private/public utilities in their response to the automation control related recommendations of the Blackout task Force Report. However, the CSSC, over time, can add considerable and effective support and supplemental assistance in the recommendation implementation phase as well as in the on-going maintenance, assurance, upgrade, and compliance to these recommendations. Furthermore, by collaborating with the appropriate power system entities responsible for recommendation implementation, the CSSC may identify future automation system security gaps not recognized in the Blackout Report and support resolution of these gaps or shortcomings.